Online Safety Policy

This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Version: [3}

Date created: [17/09/21]

Next review date: [17/09/24]

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Springfield to safeguard members of our school community online in accordance with statutory guidance and best practice.

This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Burnley Springfield Community Primary School will deal with such incidents within this policy and associated relationship policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Policy development, monitoring, and review

This Online Safety Policy has been developed by the HT, SLT and DSL governor.

Schedule for development, monitoring, and review

This Online Safety Policy was approved by the *school governing body on:*	*26th September 2023*
The implementation of this Online Safety Policy will be monitored by:	*SLT*
Monitoring will take place at regular intervals:	*Annually*
The *governing body* will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Summer term of each academic year*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*September 2024*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*DSL in the first instance*

Process for monitoring the impact of the Online Safety Policy

Springfield CPS will monitor the impact of the policy using:

- *logs of reported incidents*
- *Filtering and monitoring logs*
- *internal monitoring data for network activity*
- *surveys/questionnaires of:*
    - *learners*
    - *parents and carers*
    - *staff.*

Policy and leadership

Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals[1] and groups within the school.

Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education 2023.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff[2].
- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Governors

The DfE guidance “Keeping Children Safe in Education” states:

[2] See flow chart on dealing with online safety incidents in ‘Responding to incidents of misuse’ and relevant local authority/MAT/ HR/other relevant body disciplinary procedures.

> "Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety".
>
> "Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)"

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body".

This review will be carried out by the FGB whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor to include:

- regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- reporting to relevant *governors group/meeting*
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards
- *membership of the school Online Safety Group*

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Designated Safety Lead (DSL)- Lisette Wilson

Keeping Children Safe in Education states that:

> *"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description."*
>
> *They (the DSL) "are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college".*
>
> *They (the DSL)* "can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online".

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.

- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online.
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out.
- attend relevant governing body meetings/groups.
- report regularly to headteacher/senior leadership team
- be responsible for receiving reports of online safety incidents and handling them and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

Online Safety Lead- Mr Jordan Coates

The Online Safety Lead will:

- lead the Online Safety Group
- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL)
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments.
- have a leading role in establishing and reviewing the school online safety policies/documents.
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond.
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded, and evaluated.
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents.
- provide training and advice for staff/governors/parents/carers/learners.
- liaise with (school) technical staff, pastoral staff and support staff (as relevant)
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
    - content- being exposed to illegal inappropriate or harmful content.
    - contact- being exposed to harmful interaction with other users.
    - Conduct- online behaviour that increases the likelihood of or causes harm.
    - commerce – risks with financial implication.

Curriculum Leads- Mr Douglas/Mrs Lambert

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme.

This will be provided through:

- a discrete programme
- PHSE and SRE programmes
- A mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices.
- they understand that online safety is a core part of safeguarding.
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to Jordan Coates for investigation/action, in line with our safeguarding procedures.
- all digital communications with learners and parents/carers are on a professional level *and only carried out using official school systems.*
- online safety issues are embedded in all aspects of the curriculum and other activities.
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices.
- in lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies.
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

IT Provider

The DfE Filtering and Monitoring Standards says:

> *"Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider."*
>
> *"Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support."*
>
> *"The IT service provider should have technical responsibility for:*
>
> - *maintaining filtering and monitoring systems*
> - *providing filtering and monitoring reports*
> - *completing actions following concerns or checks to systems".*
>
> *"The IT service provider should work with the senior leadership team and DSL to:*
>
> - *procure systems.*

- *identify risk.*
- *carry out reviews.*
- *carry out checks".*

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy.
- the school technical infrastructure is secure and is not open to misuse or malicious attack.
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority or other relevant body
- there is clear, safe, and managed control of user access to networks and devices.
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to Jordan Coates for investigation and action.
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- *monitoring systems are implemented and regularly updated as agreed in school policies.*

Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy (including personal devices – where allowed)
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers

Springfield CPS will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement (the school will ask parents/carers to acknowledge these by signature)
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images.
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- *reinforcing the online safety messages provided to learners in school.*
- *the safe and responsible use of their children's personal devices in the school (where this is allowed)*

Community users

Community users who access school systems/website/learning platform as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems. (A community user's acceptable use agreement template can be found in the appendices).

Springfield CPS *encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.*

Online Safety Group

The Online Safety Group has the following members:

- Designated Safeguarding Lead – Mrs Wilson
- Online Safety Lead- Mr Coates
- Senior leader- Mr Douglas
- Online safety governor- Mr Ahmed
- Chair of Governors- Mrs Buchannan
- Technical staff- Mr Harris
- Curriculum Leads- Mr Douglas/Mrs Lambert
- Learner representatives

Members of the Online Safety Group will assist the DSL/OSL with:

- the production/review/monitoring of the school Online Safety Policy/documents.
- the production/review/monitoring of the school filtering policy and requests for filtering changes.
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage.
- reviewing network/filtering/monitoring/incident logs, where possible.
- encouraging the contribution of learners to staff awareness, emerging trends and the school online safety provision.
- consulting stakeholders – including staff/parents/carers about the online safety provision.
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.

An Online Safety Group terms of reference template can be found in the appendices.

Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

Policy

Online Safety Policy

The DfE guidance "Keeping Children Safe in Education" states:

"Online safety and the school or college's approach to it should be reflected in the child protection policy".

Our Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication.
- allocates responsibilities for the delivery of the policy.
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours.
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world.
- describes how the school will help prepare learners to be safe and responsible users of online technologies.
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms.
- is supplemented by a series of related acceptable use agreements.
- is made available to staff at induction and through normal communication channels.
- *is published on the school website*.

Acceptable use

We have defined what it regards as acceptable/unacceptable use, and this is shown in the tables below.

Acceptable use agreements

The Online Safety Policy and acceptable use agreements define acceptable use at school. The acceptable use agreements will be communicated/re-enforced through:

- staff induction and handbook
- digital signage
- posters/notices around where technology is used (where possible)
- communication with parents/carers
- built into education sessions.
- school website
- peer support.

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload,	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	• Offences relating to sexual images i.e., revenge and extreme pornography. • Incitement to and threats of violence • Hate crime. • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering. N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices. • Using penetration testing equipment (without relevant permission) N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. The National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways– further information here					X
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

deration should be given for the following activities when aken for non-educational purposes:	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Online gaming	x				x			
Online shopping/commerce	x				x			
File sharing	x				x			
Social media		x			X			
Messaging/chat		x			x			
Entertainment streaming e.g. Netflix, Disney+	X				x			
Use of video broadcasting, e.g. YouTube, Twitch, TikTok	X				x			

Mobile phones may be brought to school		x						
Use of mobile phones for learning at school	x							
Use of mobile phones in social time at school		x						
Taking photos on mobile phones/cameras	x							
Use of other personal devices, e.g. tablets, gaming devices	x							
Use of personal e-mail in school, or on school network/wi-fi	x							
Use of school e-mail for personal e-mails	x							

When using communication technologies, we consider the following as good practice:

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by school.
- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community.
- users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.

Reporting and responding

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:

> *"School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. In order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include:*
>
> - *routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse".*

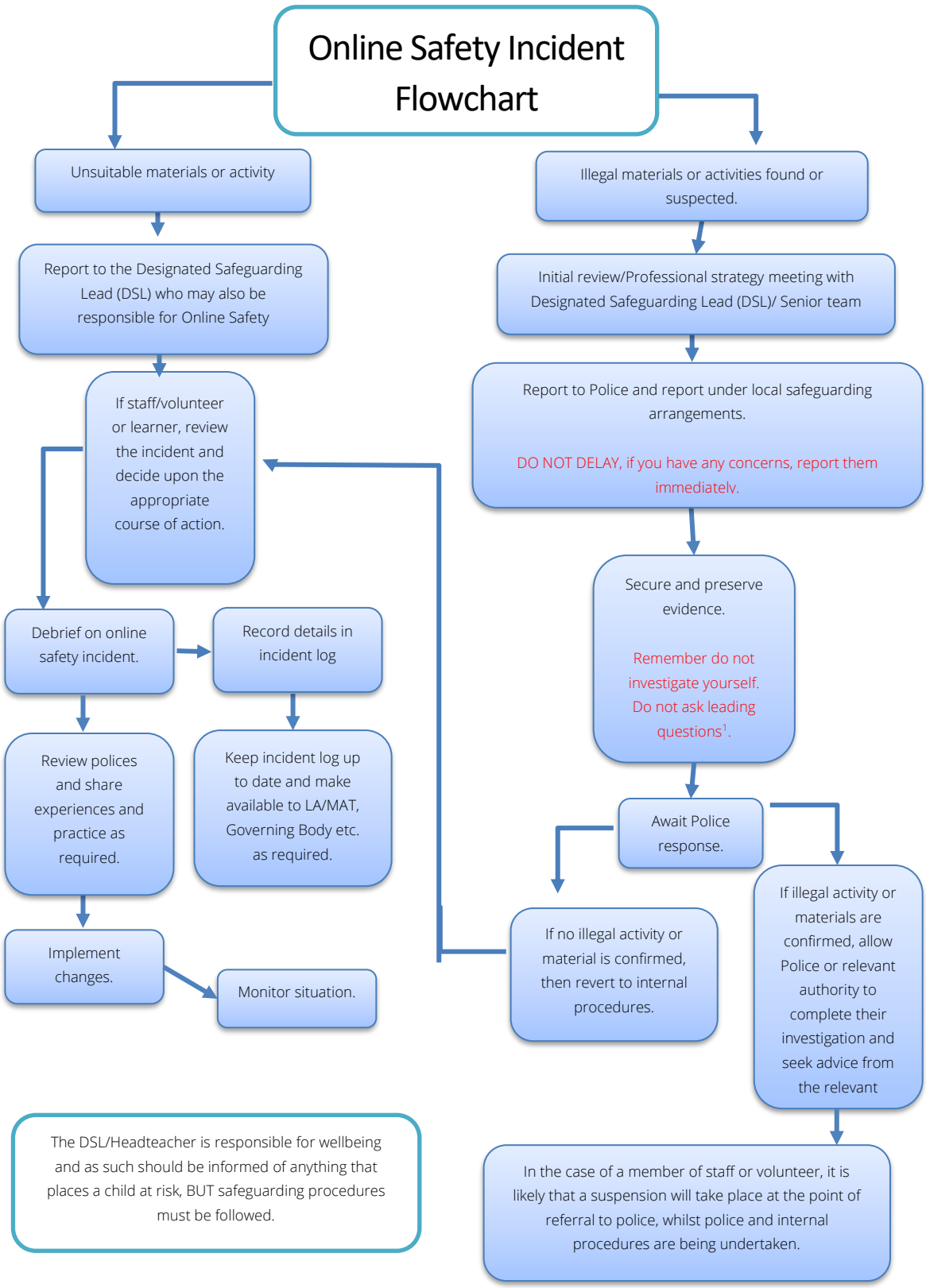
We will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. we will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies. (children have access to the online Whisper tool and in school Whisper box)
- all members of the school community will be made aware of the need to report online safety issues/incidents.
- reports will be dealt with as soon as is practically possible once they are received.
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures, this may include:
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse.
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy

- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority.
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
    - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form.
    - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
        - internal response or discipline procedures
        - involvement by local authority
        - police involvement and/or action

- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively.
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident.
- incidents should be logged.
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions.
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - *the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with:*
    - *staff, through regular briefings*
    - *learners, through assemblies/lessons*
    - *parents/carers, through newsletters, school social media, website*
    - *governors, through regular safeguarding updates*
    - *local authority/external agencies, as relevant (The Ofsted Review into Sexual Abuse in Schools and Colleges suggested "working closely with Local Safeguarding Partnerships in the area where the school or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour"*

We will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.


Online Safety Incident Flowchart
Unsuitable materials or activity
Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety
If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.
Debrief on online safety incident.
Record details in incident log
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.
Implement changes.
Monitor situation.
Illegal materials or activities found or suspected.
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions[1].
Await Police response.
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.
The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

School actions

It is more likely that we will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Responding to Learner Actions

Incidents	Refer to class teacher	Refer to Headteacher/DSL	Refer to Headteacher	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/carers	Remove device/ network/internet access rights	Issue a warning	Further sanction, in line with relationship policy.
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X	X	X					
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords		x				x			X
Corrupting or destroying the data of other users.		x				X			X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		X				x			X
Unauthorised downloading or uploading of files or use of file sharing.		x				X			X
Using proxy sites or other means to subvert the school's filtering system.		x				x			X
Accidentally accessing offensive or pornographic material and failing to report the incident.		x				X			X
Deliberately accessing or trying to access offensive or pornographic material.		X	x	x		x			X

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.		X		x		X			X
Unauthorised use of digital devices (including taking images)		X		x		x			X
Unauthorised use of online services		X		x		X			X
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		X		x		x			X
Continued infringements of the above, following previous warnings or sanctions.		x		x		x			X

Responding to Staff Actions

Incidents	Refer to line manager	Refer to Headteacher	Refer to local authority	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		X	X	X				
Deliberate actions to breach data protection or network security rules.		X				X		X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X			X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X		X				X
Using proxy sites or other means to subvert the school's filtering system.		X						X
Unauthorised downloading or uploading of files or file sharing		X						X
Breaching copyright or licensing regulations.		X				X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.		X				X		
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X				X
Using personal e-mail/social networking/messaging to carry out		X						

digital communications with learners and parents/carers								
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail		x						x
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner		x				x		
Actions which could compromise the staff member's professional standing		x				x		
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		x				x		x
Failing to report incidents whether caused by deliberate or accidental actions		x				x		
Continued infringements of the above, following previous warnings or sanctions.		x	x				x	x

Online Safety Education Programme

While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school's online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for:

> *"a carefully sequenced RSHE curriculum, based on the Department for Education's (DfE's) statutory guidance, that specifically includes sexual harassment and sexual violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of 'nudes."*

Keeping Children Safe in Education states:

> "*Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum …*"

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum for all year groups matched against a nationally agreed framework.

- Lessons are matched to need; are age-related and build on prior learning.
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes.
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc.
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Lessons and further resources are available on the CyberChoices site.
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

Note:

- *Staff should act as good role models in their use of digital technologies the internet and mobile devices.*
- *in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.*
- *where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit.*
- *it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.*

Contribution of Learners

Springfield CPS acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- *mechanisms to canvass learner feedback and opinion.*
- *appointment of digital leaders/anti-bullying ambassadors/peer mentors*
- *the Online Safety Group has learner representation.*
- *learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns.*
- *learners designing/updating acceptable use agreements.*
- *contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.*

Staff/volunteers

The DfE guidance "Keeping Children Safe in Education" states:

> "All staff should receive appropriate safeguarding and child protection training (including online safety) at induction. The training should be regularly updated. In addition, all staff should receive safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively."
>
> "Governing bodies and proprietors should ensure... that safeguarding training for staff, including online safety training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning."

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff.
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation, and the need to model positive online behaviours.
- *the Online Safety Lead and Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events, (e.g. UKSIC / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.*
- *this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.*
- *the Designated Safeguarding Lead/Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.*

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- attendance at training provided by the local authority/ or other relevant organisation.
- participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

A higher level of training will be made available to (at least) the Online Safety Governor. This will include:

- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

Families

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Springfield CPS will seek to provide information and awareness to parents and carers through:

- *regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes*
- *regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc*
- *the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.*
- *letters, newsletters, website, learning platform,*
- *high profile events / campaigns e.g. Safer Internet Day*
- *reference to the relevant web sites/publications, e.g. www.saferinternet.org.uk/; www.childnet.com/parents-and-carers (see Appendix for further links/resources).*
- *Sharing good practice with other schools in clusters and or the local authority/MAT*

Adults and Agencies

Springfield CPS will provide opportunities for local community groups and members of the wider community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- online safety messages targeted towards families and relatives.
- *providing family learning courses in use of digital technologies and online safety*
- *providing online safety information via their website and social media for the wider community*

Technology

The DfE Filtering and Monitoring Standards states that "Your IT service provider may be a staff technician or an external service provider". If the school has an external technology provider, it is the responsibility of the school to ensure that the provider carries out all the online safety and security measures that would otherwise be the responsibility of the school. It is also important that the technology provider is fully aware of the school Online Safety Policy/acceptable use agreements and the school has a Data Processing Agreement in place with them. We should also check their local authority/other relevant body policies on these technical and data protection issues if the service is not provided by the authority and will need to ensure that they have completed a Data Protection Impact Assessment (DPIA) for this contract.

Springfield CPS is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. We will ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Filtering & Monitoring

The DfE guidance (for England) on filtering and monitoring in "Keeping Children Safe in Education" states:

> "It is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the … risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified…
>
> The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards…"

Our filtering and monitoring provision (netsweeper) is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility.

The filtering and monitoring provision is reviewed at least annually by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.

- checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice.

Filtering

- Springfield CPS manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective.
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes (see Appendix for more details).
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.

- *younger learners will use child friendly/age-appropriate search engines e.g. Swiggle*
- *We have a mobile phone policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.*
- *access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.*

Monitoring

Springfield CPS has monitoring systems in place to protect the school, systems and users:

- We monitor all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

Springfield CPS follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by our risk assessment. These may include:

- physical monitoring (adult supervision in the classroom).
- internet use is logged, regularly monitored, and reviewed.
- filtering logs are regularly analysed, and breaches are reported to senior leaders.
- *where possible, school technical staff regularly monitor and record the activity of users on the school technical systems.*

Technical Security

Springfield CPS technical systems will be managed in ways that ensure that the school meets recommended technical requirements.

- **responsibility for technical security resides with SLT who may delegate activities to identified roles.**
- **all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by the SLT/Online Safety Group**
- **password policy and procedures are implemented. (consistent with guidance from the National Cyber Security Centre)**
- **the security of their username and password and must not allow other users to access the systems using their log on details.**
- **all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.**
- **all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.** (see section on passwords in 'Technical security policy template' in the Appendix C1)
- **the administrator passwords for school systems are kept in a secure place.**

- **there is a risk-based approach to the allocation of learner usernames and passwords.** (see 'Technical security policy template' in the Appendix C1 for more information)
- **there will be regular reviews and audits of the safety and security of school technical systems.**
- **servers, wireless systems and cabling are securely located and physical access restricted.**
- **appropriate security measures are in place (schools may wish to provide more detail which may need to be provided by the service provider) to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.**
- **there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,**
- **The HT is responsible for ensuring that all software purchased by and used by us is adequately licenced and that the latest software updates (patches) are applied.**
- **an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)**
- **use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them.**
- **personal use of any device on our network is regulated by acceptable use statements that a user consents to when using the network.**
- **staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider.**
- **removable media is not permitted unless approved by the SLT/IT service provider.**
- **systems are in place to control and protect personal data and data is encrypted at rest and in transit. (See school personal data policy template in the appendix for further detail)**
- **mobile device security and management procedures are in place** (where mobile devices are allowed access to school systems).
- guest users are provided with appropriate access to school systems based on an identified risk profile.

Mobile technologies

The DfE guidance "Keeping Children Safe in Education" states:

> "The school or college should have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy".

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, wearable devices, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail and data storage.

The school acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.

Springfield CPS allows:

	School devices			**Personal devices**		
	School owned for individual use	School owned for multiple users	Authorised device[3]	Student owned	Staff owned	Visitor owned
Allowed in school	**Yes**	**Yes**	**Yes**	Yes- at discretion of HT	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only	Yes	Yes	Yes	No	Yes	Yes

School owned/provided devices:

- *all school devices are managed though the use of Mobile Device Management software.*
- *there is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed.*
- *any designated mobile-free zone is clearly understood.*
- *personal use (e.g. online banking, shopping, images etc.) is clearly defined and expectations are well-communicated.*
- *the use of devices on trips/events away from school is clearly defined and expectation are well-communicated.*
- *liability for damage aligns with current school policy for the replacement of equipment.*
- *education is in place to support responsible use.*

Personal devices:

- *there is a clear policy covering the use of personal mobile devices on school premises for all users.*
- *where devices are used to support learning, staff have been trained in their planning, use and implementation, ensuring that all learners can access a required resource.*
- *where personal devices are brought to school, but their use is not permitted, appropriate, safe and secure storge should be made available.*
- *use of personal devices for school business is defined in the acceptable use policy and staff handbook. Personal devices commissioned onto our network are segregated effectively from school-owned systems.*
- *the expectations for taking/storing/using images/video aligns with the school's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted.*
- *liability for loss/damage or malfunction of personal devices is clearly defined.*
- *there is clear advice and guidance at the point of entry for visitors to acknowledge school requirements.*
- *education about the safe and responsible use of mobile devices is included in the school online safety education programmes.*

[3] Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

Social media

All schools and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race, or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

Springfield CPS provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- Ensuring that personal information is not published.
- Education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- Clear reporting guidance, including responsibilities, procedures, and sanctions.
- Risk assessment, including legal risk.
- Guidance for learners, parents/carers

School staff should ensure that:

- No reference should be made in social media to learners, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- They act as positive role models in their use of social media.

When official school social media accounts are established, there should be:

- a process for approval by senior leaders
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff.
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse.
- understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- Springfield CPS *permits reasonable and appropriate access to personal social media sites during school hours.*

Monitoring of public social media

- As part of active social media engagement, we may pro-actively monitor the Internet for public postings about the school.
- We should effectively respond to social media comments made by others according to a defined policy or process.
- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

Springfield's use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Lead to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.

The social media policy template in Appendix provides more detailed guidance on the school's responsibilities and on good practice.

Digital and video images

Springfield CPS will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- **we may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.** Guidance can be found in the DfE Safeguarding and remote education.
- **when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.**
- **staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes.**
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *learners* in the digital/video images.
- *staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images.*
- *care should be taken when sharing digital/video images that learners are appropriately dressed.*
- *learners must not take, use, share, publish or distribute images of others without their permission.*
- *photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy.*
- **learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.**
- **written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media.**

- **parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with our data protection policy.**
- **images will be securely stored in line with the school retention policy.**
- *learners' work can only be published with the permission of the learner and parents/carers.*

Online Publishing

Springfield CPS communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Social media
- Online newsletters

The school website is managed/hosted by Manchurian. Springfield CPS ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.

Springfield CPS *public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.*

Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation.

Springfield CPS:

- has a Data Protection Policy.
- implements the data protection principles and can demonstrate that it does so.
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where why and which member of staff has responsibility for managing it.
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed.
- has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed.

- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. Springfield CPS 'retention schedule" supports this.
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.
- provides staff, parents, volunteers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix)
- has procedures in place to deal with the individual rights of the data subject.
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions or entering into a relationship with a new supplier.
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors.
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data.
- reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- has a Freedom of Information Policy which sets out how it will deal with FOI requests.
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- data will be encrypted, and password protected.
- device will be password protected.
- device will be protected by up-to-date endpoint (anti-virus) software.
- data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school.
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school.
- only use encrypted data storage for personal data.
- will not transfer any school personal data to personal devices.

- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training.
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors.
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising.
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate.
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

Appendix

Copies of the more detailed template policies and agreements, contained in the appendix, can be found in the links and resources section of the relevant aspects in the 360safe self-review tool and online. The appendices are as follows:

- Learner Acceptable Use Agreement– KS2
- Learner Acceptable Use Agreement– for younger learners (Foundation/KS1)
- Parent/Carer Acceptable Use Agreement
- Staff (and Volunteer) Acceptable Use Policy Agreement
- Community Users Acceptable Use Agreement
- Online Safety Group Terms of Reference
- Harmful Sexual Behaviour Policy
- Computer Misuse and Cyber Choices Policy
- Responding to incidents of misuse – flow chart
- Record of reviewing devices/internet sites (responding to incidents of misuse)
- Reporting Log
- Training Needs Audit Log
- Technical Security Policy (including filtering and passwords)
- Personal Data Advice and Guidance
- School Online Safety Policy: Electronic Devices - Searching Screening and Confiscation (new DfE guidance from September 2022)
- Mobile Technologies Policy (inc. BYOD/BYOT)
- Social Media Policy
- Glossary of Terms

School Online Safety Policy Template Appendices

Appendices

Learner Acceptable Use Agreement– for KS2

Introduction

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open-up new opportunities for everyone. They can stimulate discussion, encourage creativity, and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended:

- to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal, and recreational use.
- to help learners understand good online behaviours that they can use in school, but also outside school.
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

When I use devices, I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my own personal safety:

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly.
- I will only visit internet sites that adults have told me are safe to visit.
- I will keep my username and password safe and secure and not share it with anyone else.
- I will be aware of "stranger danger" when I am online.
- I will not share personal information about myself or others when online.
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take a trusted adult with me.
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do.

I will think about how my behaviour online might affect other people:

- When online, I will act as I expect others to act toward me.
- I will not copy anyone else's work or files without their permission.
- I will be polite and responsible when I communicate with others, and I appreciate that others may have different opinions to me.
- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:

- I will only use my own personal devices (mobile phones/USB devices etc.) in the school if I have permission. If I am allowed, I still have to follow all the other school rules if I use them.
- I will only use social media sites with permission and at the times that are allowed.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work.

I understand that I am responsible for my actions, both in and out of school:

- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I do not follow these rules, I may be subject to disciplinary action. This may include *loss of access to the school network/internet, suspensions, parents/carers contacted and in the event of illegal activities involvement of the police.*

Learner Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner: ..... Group/Class: .....

Signed: ..... Date: .....

Parent/Carer Countersignature

Parent/Carer name: ..... Group/Class: .....

Signed: ..... Date: .....

Learner Acceptable Use Agreement – for younger learners (Foundation/KS1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of computers/tablets and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules, I might not be allowed to use a computer/tablet.

Child name: .....

Date: .....

Name of Parent: .....

Signed (parent): .....

Date: .....

Parent/Carer Acceptable Use Agreement – EYFS/KS1

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open new opportunities for everyone. They can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

Springfield Community Primary School will try to ensure that learners have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users. A copy of the learner acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

As the parent/carer of the above learners, I give permission for my son/daughter to have access to the digital technologies at school.

(EYFS/KS1)

I understand that the school has discussed the acceptable use agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Name: .....

Name of Child: .....

Signed: .....

Date: .....

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Learners and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publicly shared by any means, only your child's first name/initials will be used.

Springfield CPS will comply with the Data Protection Act and request parent's/carer's permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

Digital/Video Images Permission Form

Parent/Carers Name:..... Learner Name:.....

As the parent/carer of the above learner, I agree to the school taking digital/video images of my child/children.	Yes/No
I agree to these images being used:	
• to support learning activities.	Yes/No
• in publicity that reasonably celebrates success and promotes the work of the school.	Yes/No
• for the school website	Yes/No
• on social media- Facebook/X	Yes/No
• I agree that if I take digital or video images at, or of school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes/No

Signed: .....

Date: .....

Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal, and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.
- Springfield CPS will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are

published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

Springfield CPS has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school's ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download, or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose, or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.

When using the online systems in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.

- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: .....

Signed: .....

Date: .....

Acceptable Use Agreement for Community

This acceptable use agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices.
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices.

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, whatever the cause.
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices.
- I have read and understand the above and agree to use the school systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name: ..... Signed: ..... Date: …….

School Policy- Online Safety Group Terms of Reference

1. Purpose

To provide a consultative group that has wide representation from the Springfield community, with responsibility for issues regarding online safety and the monitoring of the online safety policy including the impact of initiatives.

2. Membership

2.1. The online safety group will seek to include representation from all stakeholders.

The composition of the group should include.

- Designated Safeguarding Lead – Mrs Wilson
- Online Safety Lead- Mr Coates
- senior leader- Mr Douglas
- Online safety governor- Mr Ahmed
- Chair of Governors- Mrs Buchannan
- Technical staff- Mr Harris
- Curriculum Leads- Mr Douglas/Mrs Lambert
- Learner representatives

Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.2. Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.3. Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature.

2.4. When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. Chairperson

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying members.
- Inviting other people to attend meetings when required.
- Guiding the meeting according to the agenda and time available.
- Ensuring all discussion items end with a decision, action or definite outcome.
- Making sure that notes are taken at the meetings and that these, with no action points, are distributed as necessary.

4. Duration of Meetings

Meetings shall be held once a half term for a period of 2 hour(s).

5. Functions

These are to assist the DSL/OSL (or other relevant person) with the following:

- To keep up to date with new developments around online safety
- To (at least) annually review and develop the online safety policy in line with new technologies and incidents.
- To monitor the delivery and impact of the online safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching/learning/training.

- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments around online safety. This could be carried out through:
    - Staff meetings
    - Governor's meetings
    - Surveys/questionnaires for learners, parents/carers and staff
    - Parents evenings
    - Website/newsletters
    - Online safety events
    - Internet Safety Day (annually held on the second Tuesday in February)
    - Other methods
        - To ensure that monitoring is carried out of Internet sites used across the schools.
        - To monitor filtering/change control logs (e.g. requests for blocking/unblocking sites).
        - To monitor the safe use of data across the schools
        - To monitor incidents involving cyberbullying for staff and learners

6. Amendments

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority. The above Terms of Reference for Burnley Springfield CPS have been agreed.

Signed by (SLT): .....

Date: .....

Date for review: .....

School Online Safety Policy- Harmful Sexual Behaviour

Statement of intent

Our school has a zero-tolerance approach to any harmful sexual behaviour involving children and acknowledge that it could be occurring at Burnley Springfield CPS and in our school community. Springfield CPS is proactive in its approach to assessing prevalence, responding to incidents and challenging and changing behaviour. This policy applies to all governors, staff and learners.

Schools have a statutory duty to safeguarding the children in their setting. We work together to foster an environment that creates healthy relationships for children and young people.

Our whole-school approach encourages healthy relationships and works to prevent harmful sexual behaviour. We provide high quality education within the curriculum to reduce the likelihood of the situations occurring.

We recognise that HSB is harmful to both the child/children affected by the behaviours and the child/children who displayed the behaviour and provide ongoing support for all involved.

Our approach is to treat everything as safeguarding incident in the first instance - we distinguish between behaviours that are exploratory and part of healthy age and ability appropriate development and those that may be harmful.

As a school we provide regular opportunities for school staff to understand what harmful sexual behaviours might look like and what they should do in the event of a report.

Related policies

This policy should be read in conjunction with:

- **Child protection and safeguarding policy**
- **Whistleblowing**
- **Relationship policy**
- **Anti-bullying policy**
- **Child on Child Abuse**
- **Online safety**
- **Acceptable Use Agreements**
- **Curriculum Policies**

Definitions

As stated in the Sexual Offences Act 2003, the term Harmful Sexual Behaviour (HSB) covers a wide range of behaviours, often these may be considered problematic, abusive, or violent and may also be developmentally inappropriate. HSB can occur online, offline or in a blend of both environments. The term HSB is widely acknowledged in child protection and should be treated in this context.

Whilst peer on peer harassment has become a widely recognised term, this has already moved towards child on child in recognition that age and development is a factor in making decisions about behaviour. A

significant age difference between the children involved in an incident may lead to a decision about the behaviour being harmful or not. For example, this could be an older child's behaviour towards a pre-pubescent child, or a younger child's behaviour towards an older child with learning difficulties. It is important that Designated Safeguarding Leads (DSL) know what is and is not HSB. DSLs should be involved in planning the curriculum for HSB, planning preventative actions and ensuring a whole-schools culture that condones HSB, alongside all other forms of abuse and harassment. This policy provides a basis for an effective approach to managing sexual violence and harassment.

What is sexual violence?

The following are sexual offences under the Sexual Offences Act 2003:

Rape: A person (A) commits an offence of rape if: he intentionally penetrates the vagina, anus or mouth of another person (B) with his penis, B does not consent to the penetration and A does not reasonably believe that B consents.

Assault by Penetration: A person (A) commits an offence if: s/he intentionally penetrates the vagina or anus of another person (B) with a part of her/his body or anything else, the penetration is sexual, B does not consent to the penetration and A does not reasonably believe that B consents.

Sexual Assault: A person (A) commits an offence of sexual assault if: s/he intentionally touches another person (B), the touching is sexual, B does not consent to the touching and A does not reasonably believe that B consents. (NOTE- Schools and colleges should be aware that sexual assault covers a very wide range of behaviour so a single act of kissing someone without consent or touching someone's bottom/breasts/genitalia without consent, can still constitute sexual assault.)

Causing someone to engage in sexual activity without consent: A person (A) commits an offence if: s/he intentionally causes another person (B) to engage in an activity, the activity is sexual, B does not consent to engaging in the activity, and A does not reasonably believe that B consents. (NOTE – this could include forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party.)

What is sexual harassment?

When referring to sexual harassment we mean 'unwanted conduct of a sexual nature' that can occur online and offline and both inside and outside of school. When we reference sexual harassment, we do so in the context of child-on-child sexual harassment. Sexual harassment is likely to: violate a child's dignity, and/or make them feel intimidated, degraded or humiliated and/or create a hostile, offensive or sexualised environment.

Whilst not intended to be an exhaustive list, sexual harassment can include:

- sexual comments, such as: telling sexual stories, making lewd comments, making sexual remarks about clothes and appearance and calling someone sexualised names.
- sexual "jokes" or taunting.
- physical behaviour, such as: deliberately brushing against someone, interfering with someone's clothes (schools and colleges should be considering when any of this crosses a line into sexual violence – it is important to talk to and consider the experience of the victim) and displaying pictures, photos or drawings of a sexual nature; and

- Online sexual harassment may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. It may include:
- consensual and non-consensual sharing of nude and semi-nude images and/or videos. Taking and sharing nude photographs of U18s is a criminal offence.
    - sharing of unwanted explicit content
    - up skirting (this is a criminal offence)
    - sexualised online bullying.
    - unwanted sexual comments and messages, including, on social media.
    - sexual exploitation; coercion and threats.

Springfield CPS consider sexual harassment in broad terms. Sexual harassment (as set out above) creates a culture that, if not challenged, can normalise inappropriate behaviours and provide an environment that may lead to sexual violence.

Responsibilities

Leaders and DSLs

Our leaders and DSLs have ultimate responsibility in dealing with all incidents of harmful sexual behaviour, including online. It is the expectation that all incidents of harmful sexual behaviour/sexual violence and harassment are reported in line with school safeguarding and child protection procedures.

We ensure that our designated safeguarding lead/s (DSL) and deputies are confident in school safeguarding processes and when it is necessary to escalate. Our DSLs know what local and national specialist support is available to support all children involved in harmful sexual behaviour and are confident as to how to access this support when required.

Designated safeguarding lead/s and their deputies have an in-depth working knowledge of key documentation, particularly KCSIE 2023 and Sexual Violence and Sexual Harassment Between Children in Schools and Colleges (DfE 2021). We ensure that they receive appropriate specialist training, commensurate with their role and that ongoing training is provided for all school staff.

It is the role of school leaders and designated safeguarding leads to ensure that all staff and Governors receive training specific to harmful sexual behaviour, and that it is included as part of induction.

Staff

It is the responsibility of all staff to have read and understood this policy and associated policies. All staff must report any incidents or suspected incidents of harmful sexual behaviour to DSLs in line with school policy and ensure they are informed of the outcome. All staff will challenge any harmful sexual language or inappropriate behaviour. Staff have a duty to ensure that the school environment is one which is safe, and which supports learners to understand safe and healthy relationships and appropriate behaviour through delivery of our curriculum.

Governors

We ensure that our governing body have a good understanding of what harmful sexual behaviour is, when it can pose a risk to children and how to keep children safe. Our governors receive regular training and

updates, both in terms of what sexualised behaviour is, but also how to effectively support establishments and their stakeholders whilst holding provision to account.

As part of the headteacher's report, our governing body has the opportunity to monitor and evaluate the approach to harmful sexual behaviour to ensure it is adequate and effective. This includes evaluation of the curriculum, pupil voice activity and evaluation of parent/carer engagement. Governors ensure that risks relating to these issues are identified, that a number of reporting routes are available, and that risks are effectively mitigated.

Learners

All learners have the right to learn in a safe, healthy and respectful school environment. Our learners benefit from a broad and balanced curriculum and are taught about healthy relationships and know how and when to report and that a range of different reporting routes is available to them. Our learners are encouraged to report any harmful sexual behaviour, even if they are not directly involved. All learners will be believed if they make a disclosure and will be treated sensitively - whilst we cannot guarantee confidentiality, their thoughts and wishes will be considered when supporting them.

Parents/carers

We work hard to engage parents and carers by:

- regular in school sessions
- sharing newsletters
- sharing information online e.g., website, social media
- providing curriculum information

Our parents and carers are made aware of how and when to report any concerns to the school, that all incidents will be handled with care and sensitivity, and that it may sometimes be necessary to involve other agencies.

Vulnerable groups

We recognise that, nationally, vulnerable learners are three times more likely to be at risk from Harmful Sexual Behaviour. These include:

- A child with additional needs and disabilities.
- A child living with domestic abuse.
- A child who is at risk of/suffering significant harm.
- A child who is at risk of/or has been exploited or at risk of exploited (CRE, CSE),
- A care experienced child.
- A child who goes missing or is missing education.
- Children who identify as, or are perceived as, LGBTQI+ and/or any of the other protected characteristics.

Children displaying HSB have often experienced their own abuse and trauma. We ensure that any vulnerable learner is offered appropriate support, both within and outside school, sometimes via specialist agencies.

Reporting

Our systems are well promoted, easily understood and easily accessible for children and young people to confidently report abuse, knowing their concerns will be treated seriously. All reports will be dealt with swiftly and sensitively and outcomes shared where appropriate. We also respond to anonymous reports, or reports made by third parties. This can be done via:

- online reporting tool,
- links to national or local organisations

Responding to an incident or disclosure

In this policy we recognise the importance of distinguishing between healthy, problematic and sexually harmful behaviour (HSB)

Our response is always based on sound safeguarding principles and follows school safeguarding processes. It is calm, considered and appropriate and puts the learner at the centre of all decisions made.

Springfield CPS will always adopt a multi-agency approach and seek external support and guidance, in line with school policy, if deemed necessary. This may include:

List relevant agencies e.g., MASH, Early Help, CAMHS, Police etc

Risk assessment

We may deem it necessary to complete a harmful sexual behaviour risk assessment as part of the response to any reported incidents. The purpose of the risk assessment is the protect and support **all those involved** by identifying potential risk, both in and out of school (e.g., including public transport, after school clubs etc) and by clearly describing the strategies put in place to mitigate such risk.

The risk assessment will be completed following a meeting with all professionals working with the learner, as well as parents or carers. Where appropriate, the learners involved will also be asked to contribute.

The risk assessment will be shared will all staff who work with the learner, as well as parents and carers. It will be dynamic and will respond to any changes in behaviour and will be regularly evaluated to assess impact.

Education

Our school's educational approach seeks to develop knowledge and understanding of healthy, problematic, and sexually harmful behaviours, and empowers young people to make healthy, informed decisions. Our school's approach is delivered predominantly through PSHE and RSE and additional opportunities are provided through:

- Cross curricular programmes
- Computing
- Assemblies

Our approach is given the time it deserves and is authentic i.e., based on current issues nationally, locally and within our setting. It is shaped and evaluated by learners and other members of the school community to ensure that it is dynamic, evolving and based on need. We do this by:

- Surveys
- Focus groups.
- Parental engagement
- Staff consultation
- Staff training

Training

It is effective safeguarding practice for the designated safeguarding lead (and deputies) to have a good understanding of HSB. This could form part of their safeguarding training. This will aid in planning preventative education, implementing preventative measures, drafting and implementing an effective child protection policy and incorporating the approach to sexual violence and sexual harassment into the whole school or college approach to safeguarding.

- Brook traffic light tool
- NSPCC training
- Whole staff training

A clear training strategy which supports staff to respond effectively to different types of harassment and sexual misconduct incidents. This should involve an assessment of the training needs of all staff. This strategy should be reviewed and evaluated on a regular basis to ensure it is fit for purpose.

Training will be made available on an ongoing basis for all staff and students to raise awareness of harassment and sexual misconduct with the purpose of preventing incidents and encouraging reporting where they do occur.

Links

Child Exploitation and Online Protection command: CEOP is a law enforcement agency which aims to keep children and young people safe from sexual exploitation and abuse. Online sexual abuse can be reported on their website and a report made to one of its Child Protection Advisors

The NSPCC provides a helpline for professionals at 0808 800 5000 and help@nspcc.org.uk. The helpline provides expert advice and support for school and college staff and will be especially useful for the designated safeguarding lead (and their deputies)

Support from specialist sexual violence sector organisations such as Rape Crisis or The Survivors Trust

The Anti-Bullying Alliance has developed guidance for schools about Sexual and sexist bullying.

The UK Safer Internet Centre provides an online safety helpline for professionals at 0344 381 4772 and helpline@saferinternet.org.uk. The helpline provides expert advice and support for school and college staff with regard to online safety issues.

Internet Watch Foundation: If the incident/report involves sexual images or videos that have been made and circulated online, the victim can be supported to get the images removed by the Internet Watch Foundation (IWF)

Childline/IWF Report Remove is a free tool that allows children to report nude or sexual images and/or videos of themselves that they think might have been shared online.

UKCIS Sharing nudes and semi-nudes advice: Advice for education settings working with children and young people on responding to reports of children sharing non-consensual nude and semi-nude images and/or videos (also known as sexting and youth produced sexual imagery).

Thinkuknow from NCA-CEOP provides support for the children's workforce, parents and carers on staying safe online.

Lucy Faithful Foundation

Marie Collins Foundation

NSPCC National Clinical and Assessment Service (NCATS)

Project deSHAME from Childnet provides useful research, advice and resources regarding online sexual harassment.

Computer Misuse and Cyber Choices Policy

All key stakeholders, including Springfield's IT service provider, have responsibility for the safeguarding of young people from computer misuse and are aware of the Cyber Choices programme led by the National Crime Agency (NCA) and managed locally by Regional Organised Crime Units (part of the national policing network). The risks to young people of crossing the line into committing cybercrimes is a safeguarding issue. This often happens without the individual even realising, young people need support in making the right #CyberChoices in their use of technology. Young people with an interest in technology, a high IQ, and an appetite to engage in risky behaviours are considered to be at a higher risk of committing a cyber offence, but many first-time offenders are also unaware of what the law governing cyber offences actually is. The average age of first-time cyber offenders in the UK has fallen significantly in recent years. The Cyber Choices programme works with individuals committing, or at risk of committing, cybercrimes which can only be carried out with technology, where devices are both the tool for committing the crime, and the target of the crime.

All staff are made aware of the safeguarding risks of computer misuse.

All staff are familiar with the NCA Hacking it Legal Leaflet*, which explains Cyber Choices and the Computer Misuse Act 1990, and lists recommended resources for teachers to use.

Staff are aware of the role of their local Regional Organised Crime Unit as their point of contact for Cyber Choices referrals.

Learners agree to the Acceptable Use Policy (AUP) which outlines acceptable online behaviours and explains that some online activity is illegal. Acceptable computer use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Lessons and further resources are available on the NCA Cyber Choices site.

Any breach of the AUP or activity by a learner that may constitute a cybercrime, in school or at home, will be referred to the Designated Safeguarding Lead for consideration as a safeguarding risk.

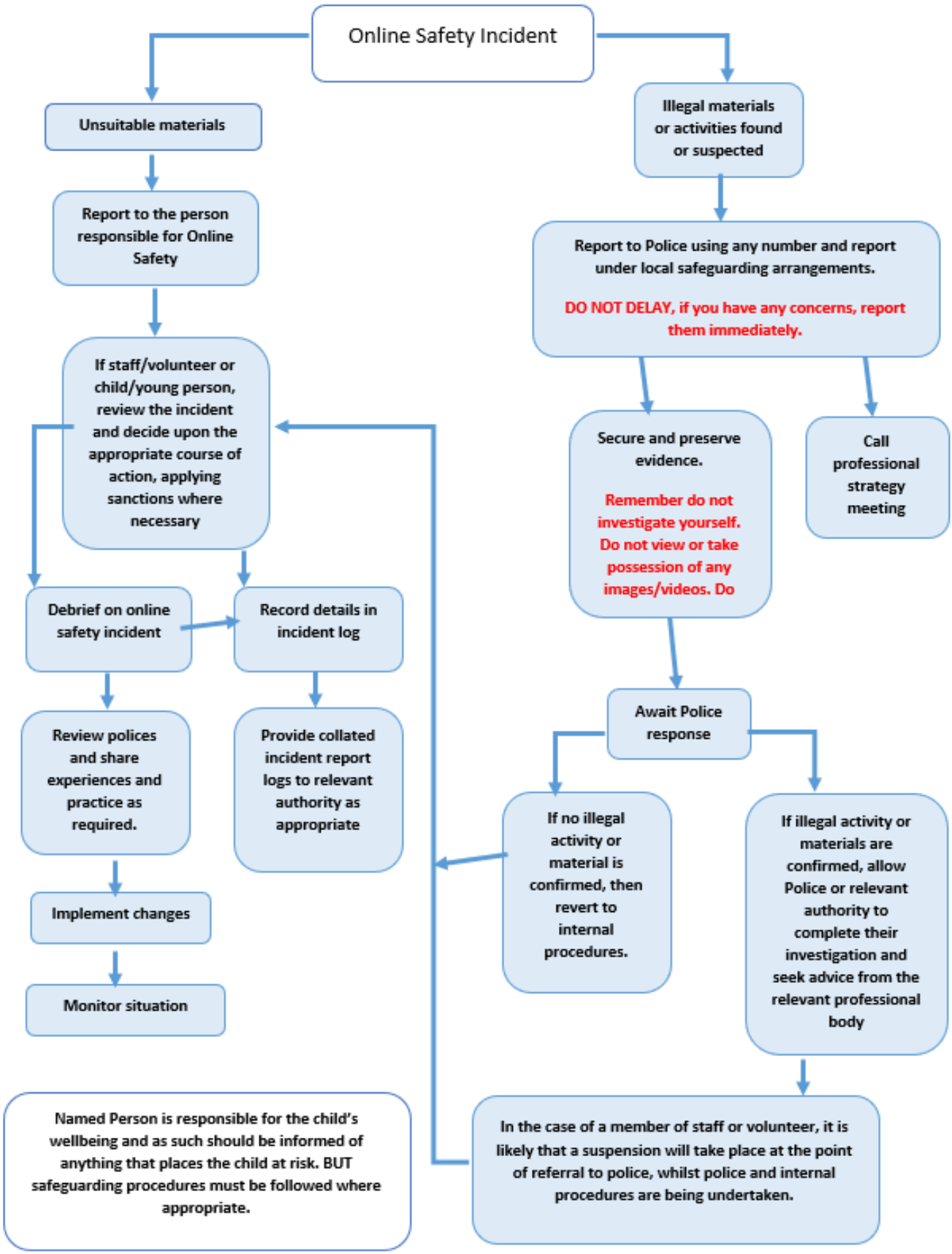
Where the DSL believes that the learner may be at risk of committing cybercrimes, or to already be committing cybercrimes, a referral to the local Cyber Choices programme will be made (contact details for all Regional Organised Crime Units are available in the "what to do if you're concerned" section at the bottom of the NCA Cyber Choices page). Where the DSL is unsure if a learner meets the referral criteria, advice should be sought from the local Cyber Choices team.

Parents also have the opportunity report potential cybercrime directly to the local Cyber Choices team but are recommended to make school-based concerns through the DSL.

The IT service provider is aware of the safeguarding requirement to refer concerns about computer misuse to the Designated Safeguarding Lead and has a clear process to follow in order to do so.

Information for parents about NCA Cyber Choices is available on the school website.

Responding to incidents of misuse – flow chart



Record of reviewing devices/internet sites (responding to incidents of misuse)

Group: .....
Date: .....
Reason for investigation: .....
.....
.....

Details of first reviewing person
Name: .....
Position: .....
Signature: .....

Details of second reviewing person
Name: .....
Position: .....
Signature: .....

Name and location of computer used for review (for web sites)
.....
.....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken.

A12 Reporting Log

Group: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

B1 Training Needs Audit Log

Group: .....

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date

School Technical Security Policy (including filtering, monitoring and passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. This is informed by the Department for Education (DfE) guidance, Keeping Children Safe in Education, and the Digital and Technology Standards and therefore applicable for schools and colleges in England. For schools and colleges outside England, this would be considered good practice, Burnley Springfield CPS should also ensure that they remain compliant with national, local authority or MAT guidance, as relevant. Burnley Springfield CPS is responsible for ensuring that the *school infrastructure/network* is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- access to personal data is securely controlled in line with the school's personal data policy.
- system logs are maintained and reviewed to monitor user activity.
- there is effective guidance and training for users.
- there are regular reviews and audits of the safety and security of school computer systems, including filtering and monitoring provision.

Responsibilities

Education settings are directly responsible for ensuring they have the appropriate level of security protection procedures in place in order to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. The management of technical security is the responsibility of Governors and Senior Leaders, supported in this by the Designated Safeguarding Lead, Online Safety Lead and IT Service Provider.

Policy statements

Burnley Springfield CPS is responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities:

- **school technical systems will be managed in ways that ensure that we meet recommended technical requirements.**
- **cyber security is included in the school risk register.**
- **there will be regular reviews and audits of the safety and security of school technical systems.**
- **servers, wireless systems, and cabling must be securely located and physical access restricted.**
- **there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,**
- **appropriate security measures (including updates) are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data, including operating systems.**
- **Springfield CPS's infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc.**

- **responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff.**
- **all users will have clearly defined access rights to school technical systems and accounts are deleted when the user leaves.** ***Details of the access rights available to groups of users will be recorded by the network manager/technical staff/other person and will be reviewed, at least annually, by the online safety group.***
- **users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.**
- **The IT Service Provider, in partnership with Governors/SLT/DSL, regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.**
- **an appropriate system is in place for users to report any actual/potential technical incident to the SLT/DSL/Online Safety Lead (OSL)/ (or other relevant person, as agreed)**
- Mr Harris is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- *by default, users do not have administrator access to any school-owned device.*
- *an agreed policy is in place regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on school devices that may be used out of school.*
- an agreed policy is in place regarding the use of removable media by users on school devices.
- personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Password Security

A safe and secure username/password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and learning platform).

Policy Statements:

- **The password policy and procedures reflect NCSC and DfE advice/guidance.**
- **The use of passwords is reduced wherever possible, for example, using Multi-Factor Authentication (MFA) or (Single Sign On) SSO.**
- **Security measures are in place to reduce brute-force attacks and common passwords are blocked.**
- **School networks and system will be protected by secure passwords.**
- **Passwords are encrypted by the system to prevent theft.**
- **Passwords do not expire, and the use of password managers is encouraged.**
- **Complexity requirements (e.g. capital letter, lower case, number, special character) are not used.**
- **Users are able to reset their password themselves.**
- **All passwords are at least 8 characters long and users are encouraged to use 3 random words.**
- **Passwords are immediately changed in the event of a suspected or confirmed compromise.**
- **No default passwords are in use. All passwords provided "out of the box" are changed to a unique password by the IT Service Provider.**

- **All accounts with access to sensitive or personal data are protected by Multi-Factor Authentication methods.**
- **A copy of administrator passwords is kept in a secure location.**
- **All users (adults and learners) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.**
- **Passwords must not be shared with anyone.**

Filtering and Monitoring

Introduction to Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, as online content changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use.

Our filtering system is operational, up to date and applied to all:

- users, including guest accounts.
- school owned devices
- devices using the school broadband connection.

Our filtering system will:

- filter all internet feeds, including any backup connections.
- be age and ability appropriate for the users and be suitable for educational settings.
- handle multilingual web content, images, common misspellings and abbreviations.
- identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them.
- provide alerts when any web content has been blocked.

Introduction to Monitoring

Monitoring user activity on our school devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software. Monitoring allows you to review user activity on school and college devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing you to take prompt action and record the outcome.

Our monitoring strategy should be informed by the filtering and monitoring review. A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access.
- individual device monitoring through software or third-party services

Filtering and Monitoring Responsibilities

DfE Filtering Standards require that schools and colleges identify and assign roles and responsibilities to manage your filtering and monitoring systems and include.

Role	Responsibility	Name / Position
Responsible Governor	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.	Mr Saf Ahmed Vice Chair and Safeguarding Governor
Senior Leadership	Team Member Responsible for ensuring these standards are met and: • procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why. • reviewing the effectiveness of your provision • overseeing reports Ensure that all staff: • understand their role. • are appropriately trained. • follow policies, processes and procedures. • act on reports and concerns	Mrs Nasim Headteacher
Designated Safeguarding Lead	Lead responsibility for safeguarding and online safety, which could include overseeing and acting on: • filtering and monitoring reports • safeguarding concerns • checks to filtering and monitoring systems	Mrs Wilson- DSL
IT Service Provider	Technical responsibility for: • maintaining filtering and monitoring systems • providing filtering and monitoring reports • completing actions following concerns or checks to systems	BT Lancs and Mr P Harris

All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:	• they witness or suspect unsuitable material has been accessed. • they can access unsuitable material. • they are teaching topics which could create unusual activity on the filtering logs. • there is failure in the software or abuse of the system. • there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks. • they notice abbreviations or misspellings that allow access to restricted material.	

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and other illegal content lists. Filter content lists are regularly updated, and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- **There is a filtering and monitoring system in place that safeguards staff and learners by blocking harmful, illegal and inappropriate content.**
- **There is a monitoring system that enables the prompt investigation of a potential safeguarding incident and outcomes are logged.**
- **Roles and responsibilities for the management of filtering and monitoring systems have been defined and allocated.**
- **The filtering and monitoring provision is reviewed at least annually and checked regularly.**
- **There is a defined and agreed process for making changes to the filtering or monitoring system that involves a senior leader in the agreement of the change.**
- **Mobile devices that access the school's internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems.**
- Springfield CPS has provided enhanced/differentiated user-level filtering through the use of the Netsweeper filtering system. (allowing different filtering levels for different ages/stages and different groups of users – staff etc.)

Changes to Filtering and Monitoring Systems

There should be a clear process for requests to change the filtering and monitoring systems and who makes the decision to alter the filtering system.

Filtering and Monitoring Review and Checks

To understand and evaluate the changing needs and potential risks of the school, the filtering and monitoring provision will be reviewed at least annually. The review will be conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and the IT service provider. Additional checks to filtering and monitoring will be informed by the review process so that governors have assurance that systems are working effectively and meeting safeguarding obligations.

Reviewing the filtering and monitoring provision

A review of filtering and monitoring will be carried out to identify the current provision, any gaps, and the specific needs of learners and staff.

The review will take account of:

- the risk profile of learners, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what the filtering system currently blocks or allows and why
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports.
- the digital resilience of learners
- teaching requirements, for example, the RHSE and PSHE curriculum
- the specific use of chosen technologies, including Bring Your Own Device (BYOD)
- what related safeguarding or technology policies are in place.
- what checks are currently taking place and how resulting actions are handled?

To make the filtering and monitoring provision effective, the review will inform:

- related safeguarding or technology policies and procedures
- roles and responsibilities
- training of staff
- curriculum and learning opportunities.
- procurement decisions
- how often and what is checked.
- monitoring strategies

The review will be carried out as a minimum annually, or when:

- a safeguarding risk is identified.
- there is a change in working practice, e.g. remote access or BYOD.
- new technology is introduced.

Checking the filtering and monitoring systems

Checks to filtering and monitoring systems are completed and recorded as part of the filtering and monitoring review process. How often the checks take place will be based on the context, the risks

highlighted in the filtering and monitoring review, and any other risk assessments. Checks will be undertaken from both a safeguarding and IT perspective.

When filtering and monitoring systems are checked this should include further checks to verify that the system setup has not changed or been deactivated. Checks are performed on a range of:

- school owned devices and services, including those used off site.
- geographical areas across the site
- user groups, for example, teachers, pupils and guests

Logs of checks are kept so they can be reviewed. This record:

- when the checks took place
- who did the check?
- what was tested or checked?
- resulting actions

Training/Awareness:

It is a statutory requirement in England that staff receive training, at least annually, about safeguarding, child protection, online safety and filtering and monitoring. Furthermore, in order to protect personal and sensitive data, governors, senior leaders, staff and learners should receive training about information security and data protection, at least annually.

Governors, Senior Leaders and staff are made aware of the expectations of them:

- at induction
- at whole-staff/governor training
- through the awareness of policy requirements
- through the acceptable use agreements
- in regular updates throughout the year

Those with specific responsibilities for filtering and monitoring (Responsible Governor, DSL, OSL or other relevant persons) will receive enhanced training to help them understand filtering and monitoring systems and their implementation and review.

Learners are made aware of the expectations of them:

- in lessons
- through the acceptable use agreements

Parents will be informed of the school's filtering policy through the acceptable use agreement and through online safety awareness sessions/newsletter etc. (amend as relevant)

Audit/Monitoring/Reporting/Review:

Governors/SLT/DSL/OSL will ensure that full records are kept of:

- Training provided.
- User Ids and requests for password changes
- *User logons*
- *Security incidents related to this policy.*
- *Annual online safety reviews including filtering and monitoring.*
- *Changes to the filtering system*
- *Checks on the filtering and monitoring systems*

School Personal Data Advice and Guidance

Suggestions for use

Data Protection Law – A Legislative Context

With effect from 25th May 2018, the data protection arrangements for the UK changed following the implementation of the European Union General Data Protection Regulation (GDPR). This represented a significant shift in legislation and in conjunction with the Data Protection Act 2018 replaced the Data Protection Act 1998.

GDPR - As a European Regulation, the GDPR has direct effect in UK law and automatically applies in the UK until we leave the EU (or until the end of any agreed transition period, if we leave with a deal). After this date, it will form part of UK law under the European Union (Withdrawal) Act 2018, with some technical changes to make it work effectively in a UK context.

Data Protection Act 2018 – this Act sits alongside the GDPR, and tailors how the GDPR applies in the UK and provides the UK-specific details such as how to handle education and safeguarding information.

No Deal Brexit -The Information Commissioner advises that in the event of a no- deal Brexit it is anticipated that the Government of the day will pass legislation to incorporate GDPR into UK law alongside the DPA 2018. Unless your school receives personal data from contacts in the EU there will be little change save to update references to the effective legislation in privacy notices etc.

In this document the term "Data Protection Law" refers to the legislation applicable to data protection and privacy as applicable in the UK from time to time.

Does the Data Protection Law apply to schools?

In short, yes. Any natural or legal person, public authority, agency or other body which processes personal data is considered a 'data controller'.

A school is, for the purposes of the Data Protection Law, a "public body" and further processes the **personal data** of numerous **data subjects** on a daily basis.

Personal data is information that relates to an identified or identifiable living individual (a data subject).

Guidance for schools is available on the Information Commissioner's Office (ICO) website including information about the Data Protection Law.

The ICO's powers are wide ranging in the event of non-compliance and schools must be aware of the huge impact that a fine or investigation will have on finances and also in the wider community for example in terms of trust.

The Data Protection Law sets out that a data controller must ensure that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to data subjects.
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are

erased or rectified without delay.

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Data Protection Law in order to safeguard the rights and freedoms of data subjects; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

These principles of the Data Protection Law drive the need for the schools to put in place appropriate **privacy notices** (to give a data subject information about the personal data processing activities, **legal basis of processing** and **data subject rights**) and policies (such as for reporting a breach, managing a data subject access request, training, retention etc.) to demonstrate compliance.

Data Mapping to identify personal data, data subjects and processing activities.

Springfield CPS and its employees will collect and/ or process a wide range of information concerning numerous data subjects and some of this information will include personal data. Further, the schools may need to share some personal data with third parties. To be able to demonstrate and plan compliance and it is important that the school has a **data map** of these activities; it can then make sure that the correct privacy notices are provided, put in place **security measures** to keep the personal data secure and other steps to avoid **breach** and also put in place data processing agreements with the third parties.

The data map should identify what personal data held in digital format or on paper records in a school, where it is stored, why it is processed and how long it is retained.

In a typical data map for a school the data subjects and personal data will include, but is not limited to:

- Parents, legal guardians, governors – and personal data of names, addresses, contact details.
- Learners - curricular / academic data e.g. class lists, learner progress records, reports, references, contact details, health and SEN reports.
- Staff and contractors - professional records e.g. employment history, taxation and national insurance records, appraisal records and references, health records

Some types of personal data are designated as '**special category**' being personal data.
"Revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".

This should be identified separately and to lawfully process special category data, you must identify both a lawful basis and a separate condition for processing special category data. You should decide and document this before you start processing the data.

Springfield CPS will need to identify appropriate lawful process criteria for each type of personal data and if this is not possible such activities should be discontinued. The lawful processing criteria can be summarised as:

(a) Consent:	the data subject has given clear consent for you to process their personal data for a specific purpose (see below for further guidance)
(b) Contract:	the processing is necessary for a contract you have with the data subject
(c) Legal obligation:	the processing is necessary for you to comply with the law (not including contractual obligations).
(d) Vital interests:	the processing is necessary to protect someone's life.
(e) Public task:	the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
(f) Legitimate interests:	the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks) Please also be aware that these criteria must be supported by a written legitimate interest assessment.

No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the data subject.

Several of the lawful purpose criteria may relate to a particular specified purpose – a legal obligation, a contract with the individual, protecting someone's vital interests, or performing your public tasks. If you are processing for these purposes then the appropriate lawful basis may well be obvious, so it is helpful to consider these first.

As a public authority, and if you can demonstrate that the processing is to perform your tasks as set down in UK law, then you are able to use the public task basis. If not, you may still be able to consider consent or legitimate interests in some cases, depending on the nature of the processing and your relationship with the data subject. There is no absolute ban on public authorities using consent or legitimate interests as their lawful basis, but the Data Protection law does restrict public authorities' use of these two criteria.

The majority of processing of personal data conducted by public authorities will fall within Article 6(1)(e) GDPR, that *"processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"* however careful consideration must be given to any processing, especially in more novel areas. As you can see, consent is just one of several possible lawful processing criteria.

Consent has changed as a result of the GDPR and is now defined as: "in relation to the processing of personal data relating to an individual, means a freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data".

This means that where a school is relying on consent as the basis for processing personal data that consent has to be clear, meaning that pre-ticked boxes, opt-out or implied consent are no longer suitable. The GDPR does not specify an age of consent for general processing, but schools should consider the capacity of learners to freely give their informed consent.

The Information Commissioner's Office (ICO) gives clear advice on when it's appropriate to use consent as a lawful base. It states:

"Consent is appropriate if you can offer people real choice and control over how you use their data and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair."

You should only use consent if none of the other lawful bases is appropriate. If you do so, you must be able to cope with people saying no (and/or changing their minds), so it's important that you only use consent for optional extras, rather than for core information the school requires in order to function. Examples.

- consent would be appropriate for considering whether a child's photo could be published in any way.

- if your school requires learner details to be stored in an MIS, it would not be appropriate to rely on consent if the learner cannot opt out of this. In this case, you could apply the public task lawful base.

Content of Privacy Notices

Privacy Notices are a key compliance requirement as they ensure that each data subject is aware of the following points when data is collected/ processed by a data controller:

- Who the controller of the personal data is.
- What personal data is being processed and the lawful purpose of this processing?
- where and how the personal data was sourced.
- to whom the personal data may be disclosed
- how long the personal data may be retained.
- data subject's rights and how to exercise them or make a complaint.

In order to comply with the fair processing requirements in data protection law, the school will inform parents/carers of all learners of the data they collect, process and hold on the learners, the purposes for which the data is held and the third parties (e.g. LA etc.) to whom it may be passed. This privacy notice will be passed to parents/carers for example in the prospectus, newsletters, reports or a specific letter / communication or you could publish it on your website and keep it updated there. Parents/carers of young people who are new to the school will be provided with the privacy notice through an appropriate mechanism.

In some circumstances you may also require privacy notices for children / learners as data subjects as children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased. The policies that explain this should be clear and age appropriate.

Data subject's right of access

Data subjects have a number of rights in connection with their personal data. They have the right:

- to be informed – Privacy Notices
- of access – Subject Access Requests
- to rectification – correcting errors
- to erasure – deletion of data when there is no compelling reason to keep it.
- to restrict processing – blocking or suppression of processing
- to portability – unlikely to be used in a school context.
- to object – objection based on grounds pertaining to their situation.
- related to automated decision making, including profiling.

Several of these could impact schools, such as the right of access. You need to put procedures in place to deal with Subject Access Requests. These are written or verbal requests to see all or a part of the personal data held by the Controller in connection with the data subject. Controllers normally have 1 calendar month to provide the information, unless the case is unusually complex in which case an extension can be obtained.

A school must not disclose personal data even if requested in a Subject Access Request.

- if doing so would cause serious harm to the individual
- child abuse data
- adoption records
- statements of special educational needs

Your school must provide the information free of charge. However, if the request is clearly unfounded or excessive – and especially if this is a repeat request – you may charge a reasonable fee.

Breaches and how to manage a breach.

Recent publicity about data breaches suffered by organisations and individuals continues to make the area of personal data protection a current and high-profile issue for schools and other organisations. It is important that the school has a clear and well understood personal data handling policy in order to minimise the risk of personal data breaches.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A breach may arise from a theft, a deliberate attack on your systems, the unauthorised or malicious use of personal data by a member of staff, accidental loss, or equipment failure. In addition:

- no school or individual would want to be the cause of a data breach, particularly as the impact of data loss on individuals can be severe, put individuals at risk and affect personal, professional or organisational reputation.
- schools are “data rich” and the introduction of electronic storage and transmission of data has created additional potential for the loss of data.
- Springfield CPS will want to avoid the criticism and negative publicity that could be generated by any personal data breach.

Schools have always held personal data on the learners in their care, and increasingly this data is held digitally and accessible not just in schools but also from remote locations. It is important to stress that the Data Protection Laws apply to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, as it is part of an overall online safety policy template, this document will place particular emphasis on data which is held or transferred digitally.

Schools will need to carefully review their policy, in the light of pertinent Local Authority regulations and guidance and changes in legislation.

All significant data protection incidents must be reported through the DPO to the Information Commissioner’s Office based upon the local incident handling policy and communication plan. The new laws require that this notification should take place within 72 hours of the breach being detected, where feasible.

If you experience a personal data breach you need to consider whether this poses a risk to people. You need to consider the likelihood and severity of any risk to people’s rights and freedoms, following the breach. When you’ve made this assessment, if it’s likely there will be a risk then you must notify the ICO, if it’s unlikely then you don’t have to report it. You do not need to report every breach to the ICO.

Springfield CPS will have a policy for reporting, logging, managing and recovering from information risk incidents, which establishes a:

- “Responsible person” for each incident
- communications plan, including escalation procedure.
- plan of action for rapid resolution
- plan of action of non-recurrence and further awareness raising

Privacy by Design and Data Protection Impact Assessments (DPIA)

Data Protection Impact Assessments (DPIA) identify and address privacy risks early on in any project so that you can mitigate them before the project goes live.

DPIAs should be carried out by Data Managers (where relevant) under the support and guidance of the DPO. Ideally you should conduct a DPIA before processing activity starts. However, some may need to be retrospective in the early stages of compliance activity.

The risk assessment will involve:

- recognising the risks that are present.
- judging the level of the risks (both the likelihood and consequences)
- prioritising the risks.

According to the ICO a DPIA should contain:

- a description of the processing operations and the purpose
- an assessment of the necessity and proportionality of the processing in relation to the purpose
- an assessment of the risks to individuals
- the measures in place to address risk, including security and to demonstrate that you comply.

Or more simply and fully:

- who did you talk to about this?
- what is going to happen with the data and how – collection, storage, usage, disposal?
- how much personal data will be handled (number of subjects)
- why you need use personal data in this way.
- what personal data (including if it's in a 'special category') are you using
- at what points could the data become vulnerable to a breach (loss, stolen, malicious)
- what the risks are to the rights of the individuals if the data was breached.
- what are you going to do in order to reduce the risks of data loss and prove you are compliant with the law.

DPIA is an ongoing process and should be re-visited at least annually to verify that nothing has changed since the processing activity started.

Secure storage of and access to data

Springfield CPS will ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

Good practice suggests that all users will use strong passwords made up from a combination of simpler words. User passwords must never be shared.

Personal data may only be accessed on machines that are securely protected. Any device that can be used to access personal data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data should only be stored on school equipment. Private equipment (i.e. owned by the users) must not be used for the storage of school personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted, and password protected.
- The device must be password protected.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Springfield CPS will set its own policy as to whether data storage on removal media is allowed, even if encrypted. Some organisations do not allow storage of personal data on removable devices.

Springfield CPS will have a clear policy and procedures for the automatic backing up, accessing and restoring of all data held on school systems, including off-site backups.

Springfield CPS will have a clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Dropbox, Microsoft 365, Google Drive) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. We will ensure that it is satisfied with controls put in place by remote / cloud-based data services providers to protect the data.

As a Data Controller, the school is responsible for the security of any data passed to a "third party". Specific data processing clauses must be included in all contracts where personal data is likely to be passed to a third party.

All paper based personal data must be held in lockable storage, whether on or off site.

Secure transfer of data and access out of school

Springfield CPS recognises that personal data may be accessed by users out of school or transferred to the local authority or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted, and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school.
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform?
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

Disposal of personal data

Springfield CPS will implement a document retention schedule that defines the length of time personal data is held before secure destruction. The Information and Records Management Society Toolkit for schools provides support for this process. Springfield CPS will ensure the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely disposed of, and other media must be shredded, incinerated or otherwise disintegrated.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Demonstrating Compliance - Audit Logging / Reporting / Incident Handling

Organisations are required to keep records of processing activity. The data map referred to above will assist here. Records must include:

- the name and contact details of the data controller
- where applicable, the name and contact details of the joint controller and data protection officer
- the purpose of the processing
- to whom the data has been/will be disclosed
- description of data subject and personal data
- where relevant the countries it has been transferred to
- under which condition for processing the personal data has been collected
- under what lawful basis processing is being carried out?
- where necessary, how it is retained and destroyed.
- a general description of the technical and organisational security measures.

Clearly, in order to maintain these records good auditing processes must be followed, both at the start of the exercise and on-going throughout the lifetime of the requirement. Therefore, audit logs will need to be kept to:

- provide evidence of the processing activity and the DPIA
- record where, why, how and to whom personal data has been shared.
- log the disposal and destruction of the personal data.
- enable the school to target training at the most at-risk data.
- record any breaches that impact on the personal data.

Fee

Springfield CPS will pay the relevant annual fee to the Information Commissioner's Office (ICO). Failure to renew may render the school to a penalty in additional to other fines possible under the Data Protection Law.

Responsibilities

Every maintained school is required to appoint a Data Protection Officer as a core function of 'the businesses.

The Data Protection Officer (DPO) can be internally or externally appointed.

They must have:

- expert knowledge
- timely and proper involvement in all issues relating to data protection.
- the necessary resources to fulfil the role.
- access to the necessary personal data processing operations
- a direct reporting route to the highest management level

The data controller must:

- not give the DPO instructions regarding the performance of tasks
- ensure that the DPO does not perform a duty or role that would lead to a conflict of interests.
- not dismiss or penalise the DPO for performing the tasks required of them.

As a minimum a Data Protection Officer must:

- inform, as necessary, the controller, a processor or an employee of their obligations under the data protection laws.
- provide advice on a data protection impact assessment.
- co-operate with the Information Commissioner
- act as the contact point for the Information Commissioner
- monitor compliance with policies of the controller in relation to the protection of personal data.
- monitor compliance by the controller with Data Protection Law

The school may also wish to appoint a Data Manager. Schools are encouraged to separate this role from that of Data Protection Officer, where possible. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment.
- oversee the System Controllers

The school may also wish to appoint System Controllers for the various types of data being held (e.g. learner information / staff information / assessment data etc.). System Controllers will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose?
- how information has been amended or added to over time, and
- who has access to the data and why.

Everyone in school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor (either in the schools or elsewhere if on school business).

Training & awareness

All staff must receive data handling awareness / data protection training and will be made aware of their responsibilities. This should be undertaken regularly. You can do this through:

- Induction training for new staff
- Staff meetings / briefings / INSET.
- Day to day support and guidance from System Controllers

Freedom of Information Act

All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests. FOI aims to increase transparency and accountability in public sector organisations as part of a healthy democratic process. Whilst FOI requests are submitted by an individual, the issue is for the school to consider whether the requested information should be released into the public domain. FOI links to Data Protection Law whenever a request includes personal data. Good advice would encourage the school to:

- delegate to the Headteacher day-to-day responsibility for FOI policy and the provision of advice, guidance, publicity and interpretation of the school's policy
- consider designating an individual with responsibility for FOI, to provide a single point of reference, coordinate FOI and related policies and procedures, take a view on possibly sensitive areas and consider what information and training staff may need.
- consider arrangements for overseeing access to information and delegation to the appropriate governing body.
- proactively publish information with details of how it can be accessed through a Publication Scheme (see Model Publication Scheme below) and review this annually.
- ensure that a well-managed records management and information system exists in order to comply with requests.
- ensure a record of refusals and reasons for refusals is kept, allowing the schools to review its access policy on an annual basis.

Model Publication Scheme

The Information Commissioner's Office provides schools and organisations with a model publication scheme which they should complete. The school's publication scheme should be reviewed annually.

The ICO produce guidance on the model publication scheme for schools. This is designed to support schools complete the Guide to Information for Schools.

Parental permission for use of cloud hosted services.

Schools that use cloud hosting services are advised to seek appropriate consent to set up an account for learners.

Use of Biometric Information

Biometric information is special category data. The Protection of Freedoms Act 2012, included measures that affect schools that use biometric recognition systems, such as fingerprint identification and facial scanning:

- For all learners in schools under 18, they must obtain the written consent of a parent before they take and process their child's biometric data.
- They must treat the data with appropriate care and must comply with data protection principles as set out in the Data Protection Law
- They must provide alternative means for accessing services where a parent or learner has refused consent.

Privacy and Electronic Communications

Schools should be aware that they are subject to the Privacy and Electronic Communications Regulations in the operation of their websites.

School Online Safety Policy: Electronic Devices - Searching Screening and Confiscation (updated with new DfE guidance – September 2022)

Introduction

The changing face of information technologies and ever-increasing learner use of these technologies has meant that the Education Acts were updated to keep pace. Part 2 of the Education Act 2011 (Discipline) introduced changes to the powers afforded to schools by statute to search learners in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the school will not face legal challenge but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.

The particular changes we deal with here are the added power to screen, confiscate and search for items 'banned under the school rules and the power to 'delete data' stored on confiscated electronic devices.

Items banned under the school rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).

An item banned by the school rules may only be searched for under these new powers if it has been identified in the school rules as an item that can be searched for. It is therefore important that there is a school policy which sets out clearly and unambiguously the items which:

- are banned under the school rules; and
- are banned AND can be searched for by authorised school staff.

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question relates to an offence and/or may be used to cause harm, to disrupt teaching or could break the school rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, **if they think there is a good reason to do so**.

Responsibilities

The Headteacher is responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups. The policies will normally be taken to Governors for approval. The Headteacher will need to authorise those staff who are allowed to carry out searches.

This policy has been written by and will be reviewed by the Headteacher.

The Headteacher has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data/files on those devices: (Mrs Wilson, Mr Coates, Mrs Staples and Mr Douglas)

The Headteacher may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

Training/Awareness

Members of staff should be made aware of the school's policy on "Electronic devices – searching, confiscation and deletion":

- at induction
- at regular updating sessions on the school's online safety policy

Members of staff authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data/files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Policy Statements

Screening

Learners are only allowed to bring mobile phones or other personal electronic devices to school and use them only within the rules laid down by the school in exceptional circumstances once permission has been sought by the Head teacher.

If learners breach these roles:

The sanctions for breaking these rules will be dealt with individually and parents informed.

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- Searching with consent - Authorised staff may search with the learner's consent for any item.
- Searching without consent - Authorised staff may only search without the learner's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for

In carrying out the search:
The authorised member of staff must have reasonable grounds for suspecting that a *learner* is in possession of a prohibited item i.e. an item banned by the school rules, and which can be searched for.

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone/personal electronic device before carrying out a search.

The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the learner being searched.

The authorised member of staff carrying out the search must be the same gender as the *learner* being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the *learner* being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a learner of the opposite gender including without a witness present, but **only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.**

Extent of the search:
The person conducting the search may not require the learner to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; jacket; gloves and scarves).

'Possessions' means any goods over which the learner has or appears to have control – this includes desks, lockers and bags.

A learner's possessions can only be searched in the presence of the learner and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

Electronic devices

The DfE guidance – Searching, Screening and Confiscation received significant updates in July 2022 and now states:

- Electronic devices, including mobile phones, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, indecent images of children, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour.
- As with all prohibited items, staff should first consider the appropriate safeguarding response if they find images, data or files on an electronic device that they reasonably suspect are likely to put a person at risk.

- Staff may examine any data or files on an electronic device they have confiscated as a result of a search. if there is good reason to do so (defined earlier in the guidance as)
    - poses a risk to staff or pupils.
    - is prohibited, or identified in the school rules for which a search can be made or
    - is evidence in relation to an offence.
- If the member of staff conducting the search suspects, they may find an indecent image of a child (sometimes known as nude or semi-nude images), the member of staff should never intentionally view the image, and must never copy, print, share, store or save such images. When an incident might involve an indecent image of a child and/or video, the member of staff should confiscate the device, avoid looking at the device and refer the incident to the designated safeguarding lead (or deputy) as the most appropriate person to advise on the school's response. Handling such reports or concerns can be especially complicated and schools should follow the principles as set out in Keeping children safe in education. The UK Council for Internet Safety also provides the following guidance to support school staff and designated safeguarding leads: Sharing nudes and semi-nudes: advice for education settings working with children and young people.
- If a member of staff finds any image, data or file that they suspect might constitute a specified offence, then they must be delivered to the police as soon as is reasonably practicable.
- In exceptional circumstances members of staff may dispose of the image or data if there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files, the member of staff must have regard to the following guidance issued by the Secretary of State
    - In determining whether there is a 'good reason' to examine the data or files, the member of staff should reasonably suspect that the data or file on the device has been, or could be used, to cause harm, undermine the safe environment of the school and disrupt teaching, or be used to commit an offence.
    - In determining whether there is a 'good reason' to erase any data or files from the device, the member of staff should consider whether the material found may constitute evidence relating to a suspected offence. In those instances, the data or files should not be deleted, and the device must be handed to the police as soon as it is reasonably practicable. If the data or files are not suspected to be evidence in relation to an offence, a member of staff may delete the data or files if the continued existence of the data or file is likely to continue to cause harm to any person and the pupil and/or the parent refuses to delete the data or files themselves.

Care of Confiscated Devices

School staff are reminded of the need to ensure the safekeeping of confiscated devices, to avoid the risk of compensation claims for damage/loss of such devices.

Audit/Monitoring/Reporting/Review

The responsible person (Mrs Wilson/ Mr Coates) will ensure that full records are kept of incidents involving the searching for and of electronic devices and the deletion of data/files.

These records will be reviewed by the Online Safety Group at regular intervals (once a half term)

This policy will be reviewed by the head teacher and governors annually and in response to changes in guidance and evidence gained from the records.

Mobile Technologies Policy

Mobile technology devices may be a school owned/provided or privately owned smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage.

The absolute key to considering the use of mobile technologies is that the learners, staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school owned/provided or personally owned. The mobile technologies policy should sit alongside a range of polices including but not limited to the safeguarding policy, anti-bullying policy, acceptable use policy, policies around theft or malicious damage and the behaviour policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Learners now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen learning, but they can also develop digital literacy, fluency and citizenship in learners that will prepare them for the high-tech world in which they will live, learn and work.

Considerations

There are a number of issues and risks to consider when implementing mobile technologies, these include security risks in allowing connections to your school network, filtering of personal devices, breakages and insurance, access to devices for all learners, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership.

The use of mobile technologies brings both real benefits and challenges for the whole school community – including teachers - and the only effective way for a school to implement these successfully is to involve the whole school community from the outset. Before the school embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

- The school acceptable use agreements for staff, learners and parents/carers will give consideration to the use of mobile technologies.
- Springfield CPS allows:

	School/devices			Personal devices		
	School owned and allocated to a single user	School owned for use by multiple users	Authorised device[4]	Learner owned	Staff owned	Visitor owned
Allowed in school	**Yes**	**Yes**	**Yes**	Yes- at discretion of HT	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only	Yes	Yes	Yes	No	Yes	Yes

Burnley Springfield CPS has provided technical solutions for the safe use of mobile technologies in school.

- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g. Internet only access, network access allowed, shared folder network access)
- Springfield CPS has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices.
- For all mobile technologies on the school network, filtering will be applied to the internet connection and attempts to bypass this are not permitted.
- Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user.
- All mobile devices on the school network are monitored.
- The software/apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps.
- Springfield CPS will ensure that devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to learners on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.
- Where a school device has been provided to support learning. It is expected that learners will bring devices to the school as required.
- The changing of settings that would stop the device working as it was originally set up and intended to work is not permitted.

When personal devices are permitted:

- *Personal devices commissioned onto the school network are segregated effectively from school-owned systems Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school.*
- *Springfield CPS accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)*
- *Springfield CPS accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues.*

[4] Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- *Springfield CPS recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Passcodes or PINs should be set on personal devices to aid security.*
- *Springfield CPS is not responsible for the day-to-day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.*

Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition:

- **there is clear advice and guidance at the point of entry for visitors to acknowledge school requirements.**
- **Users are responsible for keeping their device up to date through software, security and app updates.**
- **Users are responsible for charging their own devices and for protecting and looking after their devices while in the school.**
- **Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.**
- **Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.**
- **The expectations for taking/storing/using images/video aligns with the school's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted.**
- *Devices may be used in lessons in accordance with teacher direction.*
- *Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances*
- *Printing from personal devices will not be possible.*

Social Media Policy

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

Springfield CPS recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and learners are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the school, its staff, parents, carers and children.

Scope

This policy is subject to the school's codes of conduct and acceptable use agreements.

This policy:

- **Applies to all staff and to all online communications which directly or indirectly, represent the school.**
- **Applies to such online communications posted at any time and from anywhere.**
- Encourages the safe and responsible use of social media through training and education.
- *Defines the monitoring of public social media activity pertaining to the school.*

Springfield CPS respects privacy and understands that staff and learners may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school's name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with, or impacts on, the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with learners are also considered. *Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.*

Organisational control

Roles & Responsibilities

- **SLT**

    - Facilitating training and guidance on Social Media use.
    - Developing and implementing the Social Media policy
    - Taking a lead role in investigating any reported incidents.
    - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
    - Receive completed applications for social media accounts.
    - Approve account creation.
- **Administrator/Moderator**
    - Create the account following SLT approval.
    - Store account details, including passwords securely.
    - Be involved in monitoring and contributing to the account.
    - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
- **Staff**
    - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies.
    - Attending appropriate training
    - Regularly monitoring, updating and managing content he/she has posted via school accounts.
    - Adding an appropriate disclaimer to personal accounts when naming the school

Process for creating new accounts.

The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the Leadership Team which covers the following points: -

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed?

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

School accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention are essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- **Springfield CPS requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.**
- **Digital communications by staff must be professional and respectful at all times and in accordance with this policy**. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. *Springfield CPS permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.*
- Springfield CPS will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, we will deal with the matter internally. Where conduct is considered illegal, we will report the matter to the police and other relevant external agencies and may act according to the disciplinary policy.

Legal considerations

- **Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.**
- **Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.**

Handling abuse

- When acting on behalf of the school, respond to harmful and / or offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report, or delete other users or their comments/posts and should inform the audience exactly why the action was taken.
- If you feel that you or someone else is subject to abuse by colleagues through use of online communications, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing online content are:

- Engaging
- Conversational
- Informative

- Professional

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- **Permission to use any photos or video recordings should be sought in line with our digital and video images policy**. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- **Under no circumstances should staff share or upload learner pictures online other than via official school channels.**
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Learners should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- **Staff**
    - Personal communications are those made via a personal online account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
    - Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
    - Where excessive or inappropriate personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
    - *Springfield CPS permits reasonable and appropriate access to private social media sites.*
- **Learners**
    - **Staff are not permitted to follow or engage with current or prior learners of the school on any personal social media account.**
    - The school's education programme should enable the learners to be safe and responsible users of social media.
    - Learners are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy.
- **Parents/Carers**
    - **If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.**
    - Springfield CPS has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
    - Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- Springfield CPS should effectively respond to social media comments made by others according to a defined policy or process.

Appendix

Managing your personal use of social media:

- "Nothing" on social media is truly private.
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts.
- Check your settings regularly and test your privacy.
- Keep an eye on your digital footprint.
- Keep your personal information private.
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post.
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem.

Managing school social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school.
- Use a disclaimer when expressing personal views.
- Make it clear who is posting content.
- Use an appropriate and professional tone.
- Be respectful to all parties.
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author.
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion.
- Seek advice and report any mistakes using the school's reporting process.
- Consider turning off tagging people in images where possible.
- Ensure the account is set up securely and the account can be transferred to another approved staff member in the event of the account holder leaving the school.

The Don'ts

- Don't make comments, post content or link to materials that will bring the school into disrepute.
- Don't publish confidential or commercially sensitive material.
- Don't breach copyright, data protection or other relevant legislation.
- Don't link to, embed, or add potentially inappropriate content. Consider the appropriateness of content for any audience of school accounts.
- Don't post derogatory, defamatory, offensive, harassing, or discriminatory content.

- Don’t use social media to air internal grievances.

Glossary of Terms

AUP/AUA	Acceptable Use Policy/Agreement – see templates earlier in this document.
CEOP	Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
INSET	In Service Education and Training
IP address	the label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MAT	Multi Academy Trust
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
UKSIC	UK Safer Internet Centre – EU funded centre.
UKCIS	UK Council for Internet Safety
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol