



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: [1]

Date created: [17/09/22]

Next review date: [17/09/23]

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Burnley Springfield Community Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice. Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced as outlined in the attached 'Legislation' Appendix.

This Online Safety 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).

Burnley Springfield Community Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying 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 and SLT team

Schedule for development, monitoring and review

This Online Safety Policy was approved by the <i>school governing body</i> on:	27 th September 2022
The implementation of this Online Safety Policy will be monitored by:	<i>SLT</i>
Monitoring will take place at regular intervals:	<i>Annually</i>
The <i>governing body</i> 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:	<i>Summer term of each academic year</i>
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:	<i>September 2023</i>
Should serious online safety incidents take place, the following external persons/agencies should be informed:	<i>DSL in the first instance</i>

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- *logs of reported incidents*
- *monitoring logs of internet activity (including sites visited)*
- *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 individuals¹ 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 may be delegated to the Online Safety Lead.
- 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 staff².
- The headteacher/senior leaders are responsible for ensuring that the Online Safety Lead, 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 Online Safety Lead.

Governors

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

“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”

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”².

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 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)**
- **reporting to relevant *governors group/meeting***
- *membership of the school Online Safety Group*

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.

- *occasional review of the filtering change control logs and the monitoring of filtering logs (where possible)*

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

Online Safety Lead- Mrs Wilson

The Online Safety Lead will:

- lead the Online Safety Group
- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL), where these roles are not combined
- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- 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
- receive reports of online safety incidents³ and create a log of incidents to inform future online safety developments
- provide (or identify sources of) training and advice for staff/governors/parents/carers /learners
- liaise with (school/local authority) technical staff, pastoral staff and support staff (as relevant)
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
- attend relevant governing body meetings/groups
- report regularly to headteacher/senior leadership team.
- liaises with the local authority

Designated Safeguarding Lead (DSL)- Mrs Wilson

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

“The designated safeguarding lead should take lead responsibility for safeguarding and child protection (**including online safety**). This should be explicit in the role holder’s job description.” ... Training should provide designated safeguarding leads with a good understanding of their own role, ... so they ... 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.”

The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data ⁴
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying.

Curriculum Lead

Curriculum Lead and PSHCE lead (Mrs Staples and Mrs Lambert) will work with the Online Safety Lead (Mrs Wilson) to develop a planned and coordinated online safety education programme.

This will be provided through:

- a mix of discrete programmes
- 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 Mrs Wilson (DSL) for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers should be 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

⁴ See 'Personal data policy' in the Appendix.

- in lessons where internet use is pre-planned 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 lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies
- have 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.

Network manager- Phil

The network manager 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 the required online safety technical requirements as identified by the local authority
- 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 Mrs Wilson 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 software/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
- 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

The school 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
- publish information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning digital images, cloud services etc (see parent/carer AUA in the appendix)

- 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 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).

The school 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

- Online Safety Lead /Designated Safeguarding Lead - Mrs Wilson
- Senior leaders
- Online safety governor- Mrs Stringer
- Technical staff where required
- Curriculum Leads- Mrs Staples and Mrs Lambert

Members of the Online Safety Group will assist the Online Safety Lead with:

- the production/review/monitoring of the school Online Safety Policy/documents
- the production/review/monitoring of the school filtering policy (if possible and if the school chooses to have one) 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”

The school 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 via staff meetings
- *is published on the school website.*

Acceptable use

The school has 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 the school. The acceptable use agreements will be communicated/re-enforced through:

- staff induction and handbook
- posters/notices around where technology is used
- communication with parents/carers
- school website

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, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	<p>Any illegal activity for example:</p> <ul style="list-style-type: none"> • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • 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 					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	<ul style="list-style-type: none"> • 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) 					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	
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
	Infringing copyright				X	

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	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	

Consideration should be given for the following activities when undertaken 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								
Online shopping/commerce								
File sharing								
Social media								
Messaging/chat								
Entertainment streaming e.g. Netflix, Disney+								
Use of video broadcasting, e.g. YouTube, Twitch, TikTok								
Mobile phones may be brought to school								

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

When using communication technologies, the school considers the following as good practice:

- **when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the 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:

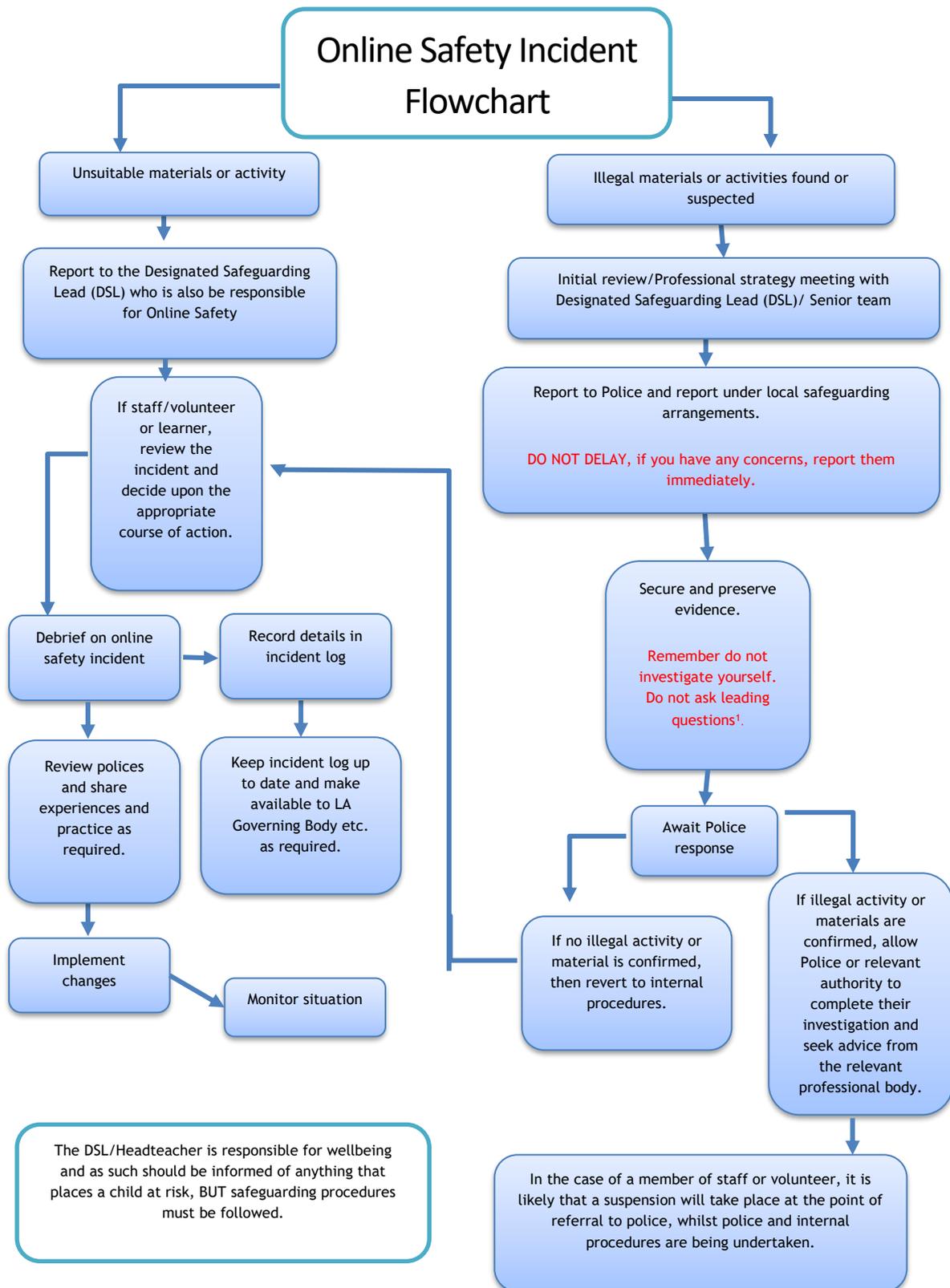
- *routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse”*

The school 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. The school 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 Whisper tool)
- **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.**
- 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. (A template reporting log can be found in the appendix).

- 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 (as relevant)
- 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 school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.



School actions

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

Responding to Staff Actions

Incidents	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		X
Unauthorised downloading or uploading of files or file sharing	X				X		X
Breaching copyright or licensing regulations.	X				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		X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X				X		X
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers	X				X		

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		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		X
Continued infringements of the above, following previous warnings or sanctions.	X	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'.."

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 and regularly taught in a variety of contexts.**
- **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.
- learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school
- 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
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

Contribution of Learners

The school 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:

- *learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns*
- *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/ Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events, 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

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
- participation in school training / information sessions for staff or parents
- A higher level of training will be made available to (at least) the Online Safety Governor.

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.

The school 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
- Sharing good practice with other schools in clusters and or the local authority

Technology

The school 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. The school 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

- the school filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
- the school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre
- access to online content and services is managed for all users
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC 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
- there is a clear process in place to deal with requests for filtering changes (see Appendix for more details).
- the school has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)
- younger learners will use child friendly/age-appropriate search engines
- filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.
- 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

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

“It is essential that governing bodies and proprietors ensure that appropriate filters 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 filters 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 school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. There is a staff lead responsible for managing the monitoring strategy and processes.
- 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
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies strategy informed by the school’s 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
- *pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.*
- *where possible, school technical staff regularly monitor and record the activity of users on the school technical systems*
- *use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)*

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements

- 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
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- **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 Network Manager (or other person) and will be reviewed, at least annually, by the Online Safety Group**

- all users (adults and learners) 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. Users must immediately report any suspicion or evidence that there has been a breach of security
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by Phil who will keep an up-to-date record of users and their usernames
- the master account passwords for the school systems are kept in a secure place, e.g. school safe.
- passwords should be long.
- records of learner usernames and passwords for learners in Key Stage 1 or younger can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. *Password complexity for younger learners may be reduced (for example 6 character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged*
- password requirements for learners at Key Stage 2 and above should increase as learners progress through school
- The bursar and Phil is responsible for ensuring that all software purchased by and used by the school 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)
- appropriate security measures are in place 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 (anti-virus) software.
- an agreed policy is in place for the provision of temporary access of ‘guests’, (e.g., trainee teachers, supply teachers, visitors) onto the school systems
- 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 that allows staff to/forbids staff from downloading executable files and installing programmes on school devices
- an agreed policy is in place regarding the use of removable media (e.g., memory sticks/CDs/DVDs) by users on school devices. Staff may only use encrypted memory sticks
- systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured.

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.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school policies including but not limited to those for safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school’s online safety education programme.

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

The school allows:

	School devices			Personal devices		
	School owned for individual use	School owned for multiple users	Authorised device ⁵	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only						
No network access						

⁵ 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

With widespread use of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of learners, the school and the individual when publishing any material online.

Expectations for teachers' professional conduct are set out in the DfE Teachers Standards but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

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.

The school 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

With school social media accounts there is:

- 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.

School 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.

Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm

- **the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.**
- **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 and in line with the schools wishes. However, this is only for their own personal use (as such use is 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. (see parents and carers acceptable use agreement in the Appendix). Permission is not required for images taken solely for internal purposes**

- 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 the school 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

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

- School website
- Social media- Facebook and Twitter
- Online newsletters

The school website is managed/hosted by **Manchurian**. The school 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.

The school 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.

The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process

Data Protection

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

The school:

- **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. The school ‘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, teenagers, 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.

The Personal Data Advice and Guidance in the appendix (B2) provides more detailed information on the school’s responsibilities and on good practice.

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

School Online Safety Policy Template Appendices

A2 Learner Acceptable Use Agreement Template - 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 could include *loss of access to the school network/internet, exclusion, 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

A3 Learner Acceptable Use Agreement Template - 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

Signed (parent) on behalf of child once above explained:

A4 Parent/Carer Acceptable Use Agreement Template

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 up 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.

The 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

Parent/Carers Name:

Learner Name:

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

(KS2 and above)

I know that my son/daughter has signed an acceptable use agreement and has 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.

(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.

Given we are collecting personal data by issuing this form, please note the following:

This form- will be printed
Who will have access to this form- administrator
Where this form will be stored. In pupil files
How long this form will be stored for. Until child leaves
How this form will be destroyed- shredded

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.

The school 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 is 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.

Given we are collecting personal data by issuing this form, please note the following:

This form- will be printed	The images
Who will have access to this form- administrator	Where the images may be published. Twitter, Facebook, the schools website, local press, etc.
Where this form will be stored- pupil files	Who will have access to the images. School, website provider, press
How long this form will be stored for- until child leaves	Where the images will be stored- deleted once used.
How this form will be destroyed- will be shredded	How long the images will be stored for- deleted once used within 24 hours
	How the images will be destroyed- deleted
	How a request for deletion of the images can be made- through contact with school- equiry@springfieldcps.lancs.sch.uk

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:	
<ul style="list-style-type: none"> • to support learning activities. 	Yes/No
<ul style="list-style-type: none"> • in publicity that reasonably celebrates success and promotes the work of the school. 	Yes/No
Insert statements here that explicitly detail where images are published by the schools	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:

Learner Acceptable Use Agreement

On the following pages we have copied, for the information of parents and carers, the learner acceptable use agreement.

A copy will be attached to the parents/carers acceptable use agreement to provide information for parents and carers about the rules and behaviours that learners have committed to by signing the form.

A5 Staff (and Volunteer) Acceptable Use Policy Agreement Template

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.

The school 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.

The school 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 management instruction, 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:

A6 Acceptable Use Agreement for Community Users Template

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.

Please note the following:

Who will have access to this form- DSL	How this form will be destroyed- shredded
Where this form will be stored- DSL file	How long this form will be stored for- when service no longer provided to school

Name: Signed: Date:.....

A7 School Policy Template - Online Safety Group Terms of Reference

1. Purpose

To provide a consultative group that has wide representation from the [schools] community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives. The group will also report regularly to the Full Governing Body.

2. Membership

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

The composition of the group should include

- SLT member/s
- Child Protection/Safeguarding officer
- Teaching staff member
- Support staff member
- Online safety coordinator (not ICT coordinator by default)
- Governor
- Parent/Carer
- ICT Technical Support staff (where possible)
- *Learner representation* - for advice and feedback. *Learner voice is essential in the make-up of the online safety group, but learners would only be expected to take part in committee meetings where deemed relevant.*

2.2. 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.

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

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

2.5. 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 committee members;
- Inviting other people to attend meetings when required by the committee;
- 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 any action points are distributed as necessary

4. Duration of Meetings

Meetings shall be held once a term for a period of 2 hour(s). A special or extraordinary meeting may be called when and if deemed necessary.

5. Functions

These are to assist the Online Safety Lead (or other relevant person) with the following:

- To keep up to date with new developments in the area of 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 schools community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through:
 - Staff meetings
 - Learner forums (for advice and feedback)
 - Governors meetings
 - Surveys/questionnaires for learners, parents/carers and staff
 - Parents evenings
 - Website/VLE/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)
- 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:

A8 School Online Safety Policy Template - Harmful Sexual Behaviour

Policy for 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. The school 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**
- **Behaviour policy**
- **Anti-bullying policy**
- **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 is already moving 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 template 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- School 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?

Keeping Children Safe in Education Guidance 2022 and the Sexual Violence and sexual harassment between children in schools and colleges state:

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/college. 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
 - upskirting (this is a criminal offence)
 - sexualised online bullying
 - unwanted sexual comments and messages, including, on social media
 - sexual exploitation; coercion and threats.

It is important that schools and colleges 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 their 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 2022 and Sexual Violence and Sexual Harassment Between Children in School (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 taken into account 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.

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.

The school 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

The school 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 to 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 with 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, pastoral/ discrete lessons, visits from outside agencies etc

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 their 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
- List other training the school has undertaken

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 should 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

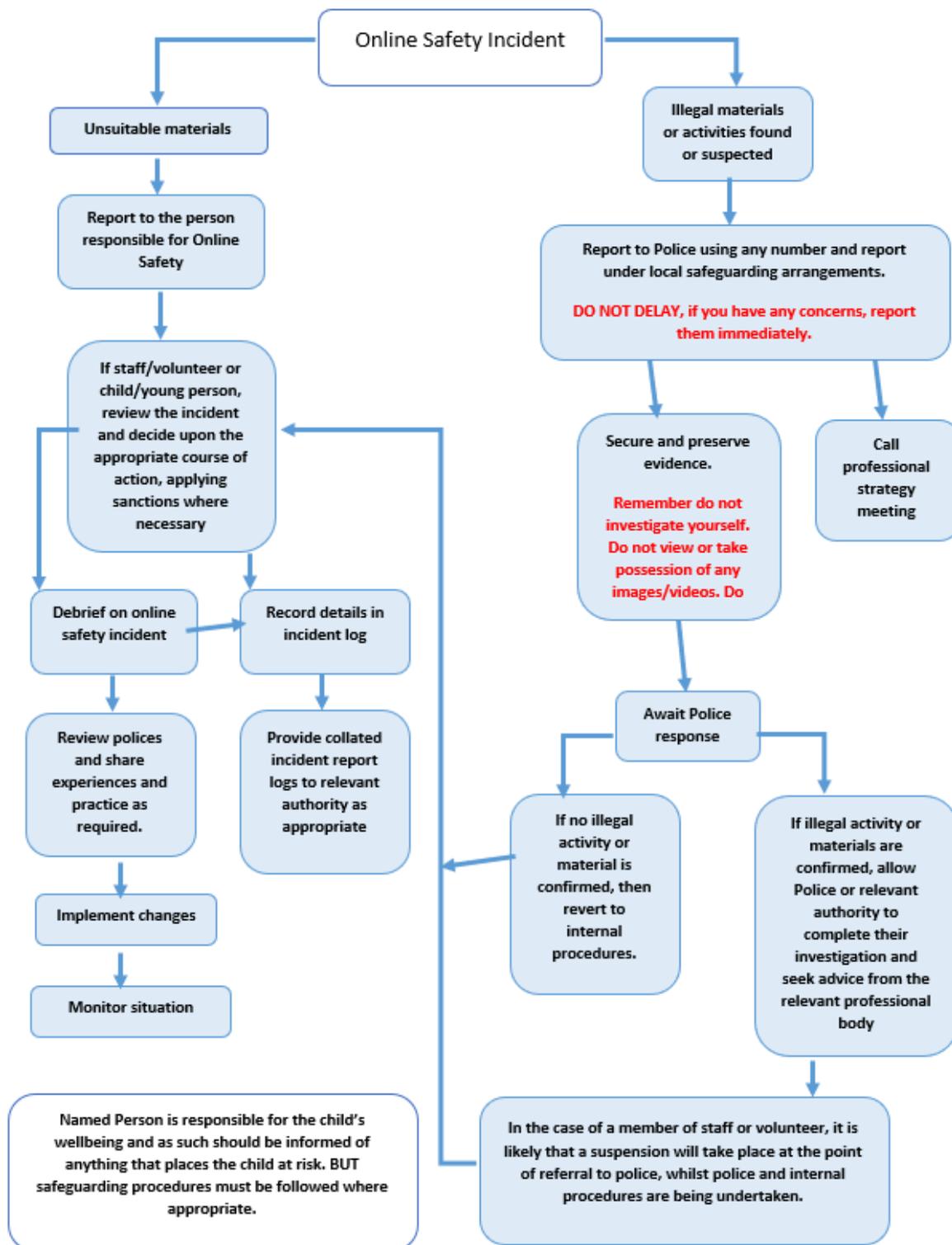
Lucy Faithful Foundation

Marie Collins Foundation

NSPCC National Clinical and Assessment Service (NCATS)

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

A9 Responding to incidents of misuse - flow chart



A10 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

A11 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

C1 School Technical Security Policy Template (including filtering 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. The school will be 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
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of Phil Harris- Easytech Support

Technical Security

Policy statements

The school will be 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 the school meets recommended technical requirements**
- **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**
- **appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data**

- 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. *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
- Phil 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
- *mobile device security and management procedures are in place*
- *school/local authority/managed service provider/technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.*
- *remote management tools are used by staff to control workstations and view users activity*
- *an appropriate system is in place for users to report any actual/potential technical incident to the online safety co-ordinator/network manager/technician (or other relevant person, as agreed)*
- an agreed policy is in place for the provision of temporary access of “guests”, (e.g. trainee teachers, supply teachers, visitors) onto the school’s systems
- *an agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by users*
- *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 (e.g. memory sticks/CDs/DVDs) by users on school devices
- the school’s infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.
- 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). You can find out more about passwords, why they are important and how to manage them in our blog article. You may wish to share this with staff members to help explain the significance of passwords as this is helpful in explaining why they are necessary and important.

Policy Statements:

- These statements apply to all users.
- All school networks and systems will be protected by secure passwords.
- 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 Network Manager (or other person) and will be reviewed, at least annually, by the online safety group (or other group).
- 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.
- All users will be provided with a username and password by the HT who will keep an up to date record of users and their usernames.

Password requirements:

- Passwords should be long. Good practice highlights that passwords over 12 characters in length are considerably more difficult to compromise than shorter passwords. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack.
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
- Passwords must not include names or any other personal information about the user that might be known by others
- Passwords must be changed on first login to the system

Learner passwords:

- Records of learner usernames and passwords for foundation phase learners can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. *Password complexity in foundation stage will be reduced. This will also apply to KS1.*
- Password requirements for learners at Key Stage 2 and above should increase as learners progress through school.
- Users will be required to change their password if it is compromised.
- Learners will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

Notes for technical staff/teams

- Each administrator should have an individual administrator account, as well as their own user account with access levels set at an appropriate level.

Consideration should also be given to using two factor authentication for such accounts.

- An administrator account password for the schools systems should also be kept in a secure place e.g. school safe. This account and password should only be used to recover or revoke access. Other administrator accounts should not have the ability to delete this account.
- Any digitally stored administrator passwords should be hashed using a suitable algorithm for storing passwords (e.g. Bcrypt or Scrypt). Message Digest algorithms such as MD5, SHA1, SHA256 etc. should not be used.
- *It is good practice that where passwords are used there is a user-controlled password reset process to enable independent, but secure re-entry to the system. This ensures that only the owner has knowledge of the password.*
- *Where user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users will be allocated by Phil Harris.*
- *Where automatically generated passwords are not possible, then a good password generator should be used by Phil Harris (IT support) to provide the user with their initial password. There should be a process for the secure transmission of this password to limit knowledge to the password creator and the user. The password should be temporary and the user should be forced to change their password on the first login.*
- *Requests for password changes should be authenticated by Phil Harris/Samaira Nasim to ensure that the new password can only be passed to the genuine user*
- **Suitable arrangements should be in place to provide visitors with appropriate access to systems which expires after use. (For example, your technical team may provide pre-created user/password combinations that can be allocated to visitors, recorded in a log, and deleted from the system after use.)**
- **In good practice, the account is “locked out” following six successive incorrect log-on attempts.**
- **Passwords shall not be displayed on screen, and shall be securely hashed when stored (use of one-way encryption).**

Training/Awareness:

Members of staff will be made aware of the school password policy:

- at induction
- through the school online safety policy and password security policy
- through the acceptable use agreement

Learners will be made aware of the school’s password policy:

- in lessons
- through the acceptable use agreement

Audit/Monitoring/Reporting/Review:

The responsible person will ensure that full records are kept of:

- User Ids and requests for password changes

- *User logons*
- *Security incidents related to this policy*

Filtering

Introduction

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, because the content on the web 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. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by BT Lancs. They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- **be logged in change control logs**
- *be reported to the Online Safety Group every month in the form of an audit of the change control logs*

All users have a responsibility to report immediately to Lisette Wilson any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

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 CAIC 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.

- *Either - The schools maintains and supports the managed filtering service provided by BT Lancs- Netsweeper*
- *The school has provided enhanced/differentiated user-level filtering through the use of the Netsweeper filtering programme. (allowing different filtering levels for different ages/stages and different groups of users - staff/learners etc.)*
- *In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).*
- *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*
- *Any filtering issues should be reported immediately to the filtering provider.*
- *Requests from staff for sites to be removed from the filtered list will be considered by the technical staff. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.*

Education/Training/Awareness

Learners will be made aware of the importance of filtering systems through the online safety education programme They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the acceptable use agreement
- induction training
- staff meetings, briefings, Inset.

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

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the school online safety policy and the acceptable use agreement. *Monitoring will take place as follows- by the lead within online safety group, Mrs Wilson- every month.*

Audit/Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- Online Safety Group
- Online Safety Governor/Governors committee
- External Filtering provider/Local Authority/Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision

Legislation

Schools should be aware of the legislative framework under which this online safety policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation.

A useful summary of relevant legislation can be found at: [Report Harmful Content: Laws about harmful behaviours](#)

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Schools may wish to view the National Crime Agency website which includes information about [“Cyber crime - preventing young people from getting involved”](#). Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful [summary of the Act on the NCA site](#).

Data Protection Act 1998

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject’s rights.
- Secure.
- Not transferred to other countries without adequate protection.

The Data Protection Act 2018:

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
 - Ascertain whether the communication is business or personal;
 - Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of learners when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

(see template policy in these appendices and for DfE guidance -

<http://www.education.gov.uk/schools/learnersupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation>)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

<https://www.gov.uk/guidance/what-maintained-schools-must-publish-online>

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Criminal Justice and Courts Act 2015

Revenge porn - as it is now commonly known - involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the [Revenge Porn Helpline](#)

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 (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust - the Regional Broadband Consortium of SW Local Authorities - is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know - educational online safety programmes for schools, young people and parents.
UKSIC	UK Safer Internet Centre - EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
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