

# FRITCHLEY CoFE (AIDED) PRIMARY AND NURSERY SCHOOL



'At Fritchley CofE (Aided) Primary and Nursery School we learn and achieve together within a safe, respectful and welcoming Christian community. Our children's spiritual and moral development is nurtured by our values, enabling them to fulfil their potential and giving them the confidence needed to be lifelong learners and problem solvers in the wider world.'

## ONLINE SAFETY POLICY

2023

## Contents

Introduction .....	2
Online Safety Policy .....	4
Scope of the Online Safety Policy .....	5
Policy development, monitoring and review .....	5
Schedule for development, monitoring and review .....	6
Process for monitoring the impact of the Online Safety Policy .....	6
Policy and leadership .....	6
Responsibilities .....	6
Online Safety Group .....	11
Professional Standards .....	12
Policy .....	12
Online Safety Policy .....	12
Acceptable use.....	13
User actions.....	13
Reporting and responding .....	17
Online Safety Incident Flowchart.....	20
Responding to Learner Actions .....	21
Responding to Staff Actions.....	23
Online Safety Education Programme .....	24
Contribution of Learners.....	25
Staff/volunteers .....	26
Governors .....	27
Families .....	27
Adults and Agencies.....	27
Technology.....	28
Filtering.....	28
Monitoring .....	28
Technical Security .....	29
Mobile technologies.....	30
Social media.....	33
Digital and video images.....	35
Online Publishing.....	36
Data Protection.....	36
Outcomes .....	38

## Introduction

This portfolio of school Online Safety Policy templates is intended to help leaders produce a suitable **Online Safety Policy** which will consider all current and relevant issues, in a whole school context, linking with other relevant policies such as a school's Safeguarding Policy, Behaviour Policy and Anti-Bullying Policy.

The requirement that learners can use digital technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Schools must, through their Online Safety Policy, meet their statutory obligations to ensure that learners are safe and are protected from potential harm, both on and off-site. It will also form part of the school's protection from legal challenge, relating to the use of digital technologies.

These policy templates suggest policy statements which, in the view of SWGfL, would be essential in any school Online Safety Policy, based on good practice. In addition, there are a range of alternative statements that schools should consider, in their particular circumstances.

An effective Online Safety Policy must be tailored to the needs of each school and an important part of the process will be the discussion and consultation which takes place during the writing or review of the policy. It is best practice that the school reviews their Online Safety Policy at least annually and, if necessary, more frequently in response to any significant new technological developments.

The DfE Keeping Children Safe in Education statutory guidance requires Local Authorities, Multi Academy Trusts, and schools in England to ensure learners are safe from harm:

*"It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to **online safety** empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate"*

*"Governing bodies and proprietors should ensure **online safety** is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how **online safety** is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement"*

The DfE Keeping Children Safe in Education guidance also recommends:

***Reviewing online safety** ... Technology, and risks and harms related to it, evolve, and change rapidly. Schools and colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their*



*children face. A free online safety self-review tool for schools can be found via the 360 safe self-review tool.*

Schools in England are subject to an increased level of scrutiny of their online safety practices by Ofsted Inspectors during inspections, while the Counter Terrorism and Securities Act 2015 requires schools to ensure that children and young people are safe from terrorist and extremist material on the internet.

With its optional statements and guidance notes, this portfolio of templates is longer than the resulting policy document is likely to be. It is intended that, while covering this complex and ever-changing issue, the resulting policy document should be concise and easily understood if it is to be effective and adopted by all. The templates are based on current best practice policies and procedures and schools can amend them to suit their requirements.

# Fritchley CofE (Aided) Primary and Nursery School

## 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: [June 2023]

Next review date: [June 2024]

## Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Fritchley CofE (Aided) Primary and Nursery 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).**

Fritchley CofE (Aided) Primary and Nursery 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 *Online safety Lead & Teaching, Learning and Community Committee* made up of:

- *headteacher/senior leaders*
- *online safety lead*
- *staff – including teachers/technical staff*
- *governors*
- *parents and carers*

## Schedule for development, monitoring and review

This Online Safety Policy was approved by the <i>school governing body</i> on:	<i>13.06.2023</i>
The implementation of this Online Safety Policy will be monitored by:	<i>Senior Leadership Team</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>Annually</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>Summer 2024</i>
Should serious online safety incidents take place, the following external persons/agencies should be informed:	<i>LA safeguarding officer (Starting Point), police</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 individuals<sup>1</sup> 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 staff<sup>2</sup>.
- 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”.

---

<sup>1</sup> In a small school some of the roles described may be combined, though it is important to ensure that there is sufficient ‘separation of responsibility’ should this be the case.

<sup>2</sup> 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.



This review will be carried out by the Teaching, Learning and Communities Committee 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***
- ***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 (Safeguarding Lead)

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 incidents<sup>3</sup> 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/MAT/external provider) 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/MAT/relevant body.

---

<sup>3</sup> [The school will need to decide how these incidents will be dealt with and whether the investigation/action will be the responsibility of the online safety lead or another member of staff, e.g. headteacher / senior leader / Designated Safeguarding Lead / class teacher / head of year, etc.](#)

## Designated Safeguarding Lead (DSL)

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 <sup>4</sup>
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying.

## Curriculum Leads

Curriculum Leads will work with the Online Safety Lead to develop a planned and coordinated online safety education programme.

This will be provided through:

- PHSE and SRE programmes
- through relevant national initiatives and opportunities e.g. [Safer Internet Day](#) and [Anti-bullying week](#).
- Embedded within computing lessons

## 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 Headteacher 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

---

<sup>4</sup> 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 and should take note of the guidance contained in the [SWGfL Safe Remote Learning Resource](#)
- 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/technical staff

NOTE: If the school has a technology service provided by an outside contractor, it is the responsibility of the school to ensure that the provider carries out all the online safety measures that the school's obligations and responsibilities require. It is also important that the provider follows and implements school Online Safety Policy and procedures.

The network manager/technical staff is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the local authority/MAT or other relevant body
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to Louise Shaw 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

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

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
- 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*

## Online Safety Group

The Online Safety Group has the following members:

- Online Safety Lead
- Designated Safeguarding Lead
- senior leaders
- online safety governor
- technical staff
- teacher and support staff members
- learners
- parents/carers
- community representatives

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
- 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

An Acceptable Use Agreement is a document that outlines a school's expectations on the responsible use of technology by its users. In most schools they are signed or acknowledged by their staff as part of their conditions of employment. Some may also require learners and parents/carers to sign them, though it is more important for these to be understood and followed rather than just signed. There is a range of acceptable use agreements in the appendices.

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
- built into education sessions
- school website

Schools should discuss and agree which activities are acceptable/unacceptable. This will vary with the size/structure of the school and the ages of the learners. It is recommended that the school discuss and agree on these activities and to complete the following tables as guidance for members of the school community:

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><b>Any illegal activity for example:</b></p> <ul style="list-style-type: none"> <li>• Child sexual abuse imagery*</li> <li>• Child sexual abuse/exploitation/grooming</li> <li>• Terrorism</li> <li>• Encouraging or assisting suicide</li> <li>• Offences relating to sexual images i.e., revenge and extreme pornography</li> <li>• Incitement to and threats of violence</li> <li>• Hate crime</li> <li>• Public order offences - harassment and stalking</li> <li>• Drug-related offences</li> <li>• Weapons / firearms offences</li> </ul>					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	<ul style="list-style-type: none"> <li>Fraud and financial crime including money laundering</li> </ul> <p>N.B. Schools should refer to guidance about dealing with self-generated images sexting – <a href="#">UKSIC Responding to and managing sexting incidents</a> and <a href="#">UKCIS – Sexting in schools and colleges</a></p>					
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	<ul style="list-style-type: none"> <li>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)</li> <li>Gaining unauthorised access to school networks, data and files, through the use of computers/devices</li> <li>Creating or propagating computer viruses or other harmful files</li> <li>Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)</li> <li>Disable/Impair/Disrupt network functionality through the use of computers/devices</li> <li>Using penetration testing equipment (without relevant permission)</li> </ul> <p>N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways – further information <a href="#">here</a></p>					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	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	

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

Consideration should be given for the following activities when undertaken for non-educational purposes:  Schools may wish to add further activities to this list.	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Online gaming	X				X			



Online shopping/commerce				X	X			
File sharing		X			X			
Social media	X				X			
Messaging/chat - ClassDojo		X			X			
Entertainment streaming e.g. Netflix, Disney+		X			X			
Use of video broadcasting, e.g. YouTube, Twitch, TikTok		X			X			
Mobile phones may be brought to school		X					X	
Use of mobile phones for learning at school	X				X			
Use of mobile phones in social time at school		X			X			
Taking photos on mobile phones or personal cameras	X				X			
Use of other personal devices, e.g. tablets, gaming devices	X				X			
Use of personal e-mail in school, or on school network/wi-fi	X				X			
Use of school e-mail for personal e-mails	X				X			

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:

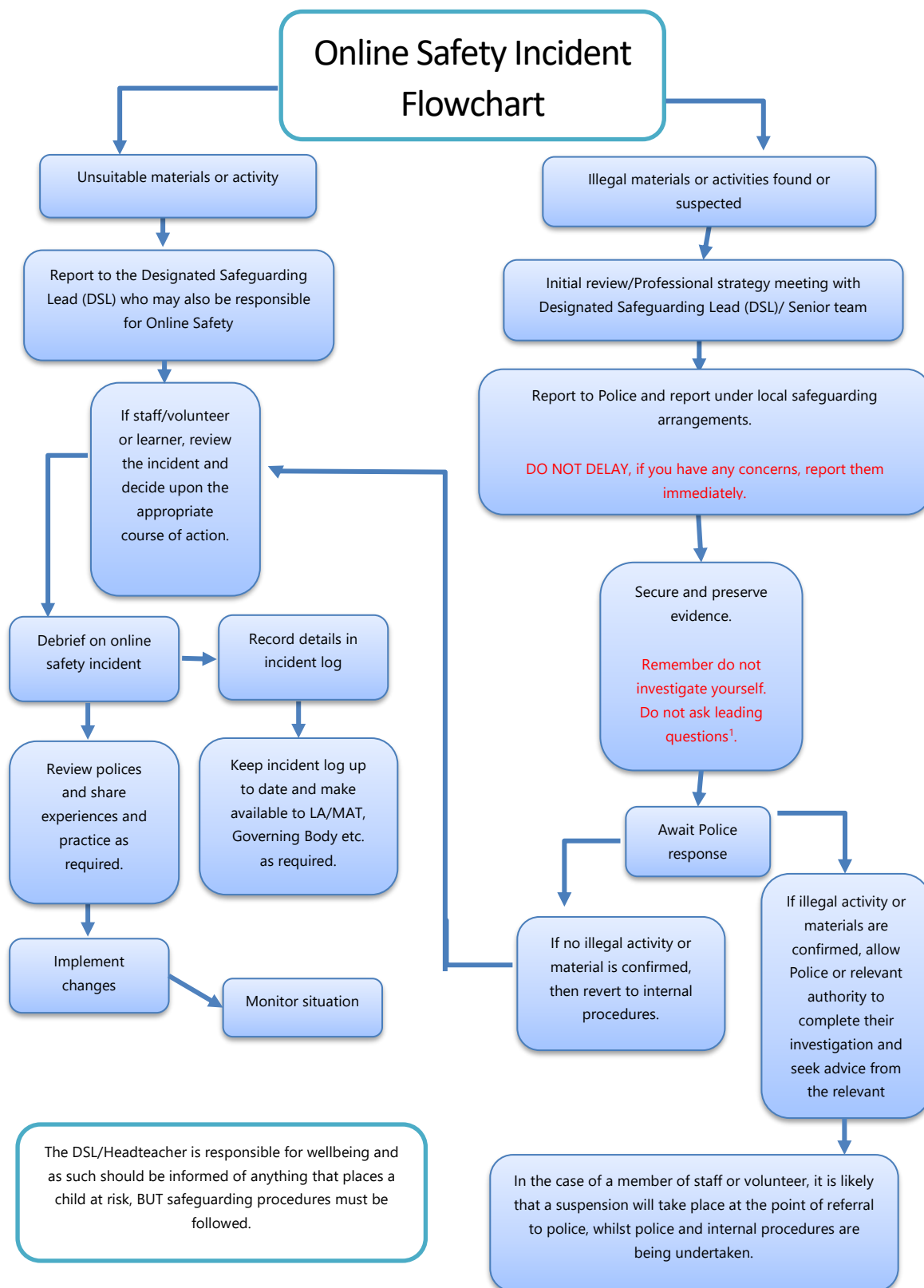
- **there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.**
- **all members of the school community will be made 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 / MAT
- 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 / MAT (as relevant)
  - 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 Ofsted Review into Sexual Abuse in Schools and Colleges suggested "working closely with Local Safeguarding Partnerships in the area where the school or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour"](#))*

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 the 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: (the school will need to agree upon its own responses and place the ticks in the relevant columns. They may also wish to add additional text to the column(s) on the left to clarify issues. Schools have found it useful to use the charts below at staff meetings/training sessions)

## Responding to Learner Actions

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

	Refer to class teacher/tutor	Refer to Assistant Headteacher	Refer to Headteacher	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/carers	Remove device/network/internet access rights	Issue a warning	Further sanction, in line with behaviour policy
Accidentally accessing offensive or pornographic material and failing to report the incident.			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					
Unauthorised use of digital devices (including taking images)		X	X						X
Unauthorised use of online services		X	X						
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		X	X			X		X	X
Continued infringements of the above, following previous warnings or sanctions.			X			X	X		

## Responding to Staff Actions

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



	Refer to Assistant Headteacher	Refer to Headteacher	Refer to local authority/MAT/HR	Refer to Police	Refer to LA / Technical Support Staff for action re	Issue a warning	Suspension	Disciplinary action
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers	X	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		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

## 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 (statements may need to be adapted, depending on school structure and the age of the learners).

- **A planned online safety curriculum for all year groups matched against a nationally agreed framework and regularly taught in a variety of contexts. This work is embedded in the scheme - Teach Computing**
- **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:

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

## Staff/volunteers

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

"All staff should receive appropriate safeguarding and child protection training (**including online safety**) at induction. The training should be **regularly updated**. In addition, all staff should receive safeguarding and child protection (**including online safety**) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively."

"Governing bodies and proprietors should ensure... that safeguarding training for staff, **including online safety** training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning."

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

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

## Governors

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

- attendance at training provided by the local authority/MAT or other relevant organisation (e.g., SWGfL)
- participation in school training / information sessions for staff or parents ([this may include attendance at assemblies/lessons](#)).

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

## 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*
- *high profile events / campaigns e.g. [Safer Internet Day](#)*
- *reference to the relevant web sites/publications, e.g. [SWGfL](#); [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/); [www.childnet.com/parents-and-carers](http://www.childnet.com/parents-and-carers) (see Appendix for further links/resources).*
- *Sharing good practice with other schools in clusters and or the local authority/MAT*

## Adults and Agencies

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

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

## 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 should 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 [Appropriate filtering](#).
- 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 provided differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff & learners.)
- younger learners will use child friendly/age-appropriate search engines e.g. [SWGfL Swiggle](#)
- filtering logs are regularly reviewed and breaches are then acted upon.
- 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.

If necessary, the school will seek advice from, and report issues to, the SWGfL [Report Harmful Content](#) site.

## 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

## 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,** [\(this is good practice in helping to prevent loss of data from ransomware attacks\)](#)
- **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 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 Louise Shaw 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 requirements for learners at Key Stage 2 and above should increase as learners progress through school
- Brent Wallhead (ICT technician) 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 that 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.
- systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured. ([See school personal data policy template in the appendix for further detail](#))

## 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.

In preparing a mobile technologies policy the school should consider possible issues and risks. These may include:

- security risks in allowing connections to your school network
- filtering of personal devices
- breakages and insurance
- access to devices for all learners
- avoiding potential classroom distraction
- network connection speeds, types of devices
- charging facilities
- total cost of ownership.

A range of mobile technology strategies is possible. However, these need to be thoroughly researched, risk assessed and aligned with existing policy prior to implementation.

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

The school allows: (the school should complete the table below to indicate which devices are allowed and define their access to school systems).

	School devices			Personal devices		
	School owned for individual use	School owned for multiple users	Authorised device <sup>5</sup>	Student owned	Staff owned	Visitor owned

<sup>5</sup> 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.



Allowed in school	Yes	Yes	Yes	Yes	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only	Yes	Yes	Yes	No	No	No
No network access	Yes	Yes	Yes	Yes	Yes	Yes

Aspects that the school may wish to consider and include in their Online Safety Policy, mobile technologies policy or acceptable use agreements should include the following:

#### School owned/provided devices:

- *to whom they will be allocated*
- *where, when and how their use is allowed – times/places/in/out of school (n.b. the need for some areas to be clearly identified as mobile free zones)*
- *if personal use is allowed*
- *levels of access to networks/internet (as above)*
- *management of devices/installation of apps/changing of settings/monitoring*
- *network/broadband capacity*
- *technical support*
- *filtering of devices*
- *access to cloud services*
- *use on trips/events away from school*
- *data protection*
- *taking/storage/use of images*
- *exit processes, what happens to devices/software/apps/stored data if user leaves the school*
- *liability for damage*
- *staff training.*

#### Personal devices

- *which users are allowed to use personal mobile devices in school (staff/learners/visitors)*
- *restrictions on where, when and how they may be used in school*
- *if used in support of learning, how staff will plan their lessons around the potential variety of device models and different operating systems*
- *storage*
- *whether staff will be allowed to use personal devices for school business*
- *levels of access to networks/internet (e.g., access, or not, to internet/guest wi-fi/network)*
- *network/broadband capacity*
- *technical support (this may be a clear statement that no technical support is available)*

- *filtering of the internet connection to these devices and monitoring the access*
- *management of software licences for personally owned devices.*
- *data protection*
- *taking/storage/use of images*
- *liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility)*
- *identification/labelling of personal devices*
- *how visitors will be informed about school requirements*
- *how education about the safe and responsible use of mobile devices is included in the school online safety education programmes*
- *how misuse will be dealt with*

## 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

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

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

### Personal use

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

### Monitoring of public social media

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

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.

The social media policy template in Appendix C4 provides more detailed guidance on the school's responsibilities and on good practice.

## 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 ([select/delete as appropriate](#)):

- **the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.** [Guidance can be found on the SWGfL Safer Remote Learning web pages and in the DfE Safeguarding and remote education](#)
- **when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.**
- **staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes**
- in accordance with [guidance from the Information Commissioner's Office](#), parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use 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 [\(amend as necessary\)](#):

- Public-facing website
- Online newsletters
- ClassDojo

The school website is managed/hosted by eSchools. 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
- has procedures in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them
- 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.



SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice, and guidance have contributed to the development of this school Online Safety Policy template and of the 360 safe online safety self-review tool:

Copyright of these policy templates is held by SWGfL. Schools and other educational institutions are permitted free use of the policy templates for the purposes of policy review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL ([onlinesafety@swgfl.org.uk](mailto:onlinesafety@swgfl.org.uk)) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in September 2022. However, SWGfL cannot guarantee it's accuracy, nor can it accept liability in respect of the use of the material.

© SWGfL 2022



# School Online Safety Policy Template Appendices

## Appendices

A1 - Learner Acceptable Use Agreement Template – for older learners

A2 - Learner Acceptable Use Agreement Template – KS2

A3 - Learner Acceptable Use Agreement Template – for younger learners (Foundation/KS1)

A4 - Parent/Carer Acceptable Use Agreement Template

A5 - Staff (and Volunteer) Acceptable Use Policy Agreement Template

A6 - Community Users Acceptable Use Agreement Template

A7 – Online Safety Group Terms of Reference Template

A8 - Harmful Sexual Behaviour Policy Template (new template added September 2022)

A9 - Responding to incidents of misuse – flow chart

A10 - Record of reviewing devices/internet sites (responding to incidents of misuse)

A11 - Reporting Log

B1 - Training Needs Audit Log

C1 - Technical Security Policy Template (including filtering and passwords)

C2 - Personal Data Advice and Guidance

C3 - School Online Safety Policy Template: Electronic Devices - Searching Screening and Confiscation  
(new DfE guidance from September 2022)

C4 - Mobile Technologies Policy Template (inc. BYOD/BYOT)

C5 - Social Media Policy Template

Legislation

Links to other organisations and resources

Glossary of Terms

## Learner Acceptable Use Agreement – for KS2

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 not use my own personal devices (mobile phones/USB devices etc.) in the school.
- I will not use social media sites.
- 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.

#### 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 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 .....

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

This is how we stay safe when we use computers:

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

Signed (child): .....

Signed (parent): .....

## Parent/Carer Acceptable Use Agreement

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.

### **Either: (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.*

### **Or: (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.

Signed: .....

Date: .....

## Staff (and Volunteer) 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 warning, a suspension, referral to Governors/Trustees and/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: .....

## School Policy – 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. Depending on the size or structure of the schools this group may be part of the safeguarding group. 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 (N.B. in small schools one member of staff may hold more than one of these posts): [add/delete where appropriate]

- 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)
- Community users (where appropriate)
- *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 [insert frequency] for a period of [insert number] 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 [add/delete where relevant]:

- 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 [add/delete as relevant]:
  - 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/uN.B.locking sites).
- To monitor the safe use of data across the schools
- To monitor incidents involving cyberbullying for staff and learners

#### 6. Amendments

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

Signed by (SLT): ..... Date: .....

Date for review: .....

## School Online Safety Policy – Harmful Sexual Behaviour

### Background context and legislation.

#### Introduction

The South West Grid for Learning Trust (SWGfL) is a charity that has been at the forefront of supporting schools with online safety and security for 20 years and was recognised as a world leader in online safety innovation in a DCMS report.

The Harmful Sexual Behaviour Support Service (HSBSS) for England was created at the start of 2022. HSBSS is a unique project, funded by the UK Home Office in response to the Everyone's Invited revelations and the subsequent reviews by Ofsted. Drawing upon our existing expertise in supporting victims of online harm we fast-tracked the creation of the service within 14 working days of the request. We work in partnership with the Marie Collins Foundation. We have a current and up-to-date understanding about how online sexual harassment manifests in schools. Overwhelmingly we speak with safeguarding leads about often complex cases involving children and young people in their school.

#### Legislative background and context

##### Key Documents:

- Department for Education: Keeping Children Safe in Education
- Department for Education: Sexual violence and sexual harassment between children in schools and colleges
- Everyone's Invited
- Department for Education: Sharing Nudes and Semi-Nudes: Advice for Education Settings working with Young People
- Ofsted: Review of sexual abuse in schools and colleges
- Department for Education: Teaching Online Safety in Schools
- Department for Education: Working together to safeguard children
- Report Harmful Content: Laws about harmful behaviours

In March 2021 it was discovered that the Everyone's Invited website was holding "testimonials" about incidents that occurred in over 3000 schools in the UK. This highlighted a wide range of abuse scenarios involving children abusing other children. As a result, the Education Secretary requested a rapid review into sexual abuse in schools and colleges in England. Ofsted published their findings in June 2021. This led to a series of recommendations for schools, multi-agency partners and government.

Ofsted's School Inspection Handbook states that:

“leaders ensure that their school’s culture addresses harmful sexual behaviour.  
**Inspectors will expect schools to assume that sexual harassment, online sexual abuse and sexual violence are happening in the community, and potentially in the school, even when there are no specific reports, and put in place a whole-school approach to address them.”**

“Schools should have appropriate and well-communicated school-wide policies in place that make it clear that sexual harassment, online sexual abuse and sexual violence (including sexualised language) are unacceptable.”

Ofsted will:

- Request that college leaders supply records and analysis of sexual harassment and sexual violence, including online, to inspectors. The Independent Schools Inspectorate will also specifically request schools to provide the same records upon notification of inspection, in addition to its current practice.
- Speak with groups of pupils, where this helps them to better understand a school or college’s approach to tackling sexual harassment and violence, including online.
- Feed this part of the inspection into a judgement of safeguarding and leadership and management. If a school’s processes are not adequate, Ofsted is likely to judge both their safeguarding practices and leadership and management as inadequate.

Your behaviour and safeguarding/child protection policies will likely be checked to see whether they set out clear and effective procedures to prevent and respond to incidents. It will be expected that you have a zero-tolerance approach to all harmful sexual behaviour.

This document has been created as a template for school leaders to assist them in creating their own Harmful Sexual Behaviour Policy.

Within this template, sections which include information or guidance are shown in BLUE. It is anticipated that schools/academies would remove these sections from their completed policy document, though this will be a decision for the group that produces the policy.

*Where sections in the template are written in ITALICS it is anticipated that schools would wish to consider whether or not to include that section or statement in their completed policy.*

**Where sections are highlighted in BOLD, it is suggested that these should be an essential part of a school/academy policy.**

## Online:

Schools and colleges should recognise that sexual violence and sexual harassment occurring online (either in isolation or in connection with face-to-face incidents) can introduce a number of complex factors. Amongst other things, this can include widespread abuse or harm across social media platforms that leads to repeat victimisation. Online concerns can be especially complicated and support is available from a range of organisations – see the links section. For this reason, schools

should ensure they have a robust, up-to-date and comprehensive online safety policy which links to other relevant safeguarding policies.

## 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 (*insert name of school*) 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 and colleges 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- Schools and colleges should be aware that sexual assault covers a very wide range of behaviour so a single act of kissing someone without consent, or touching someone's bottom/breasts/genitalia without consent, can still constitute sexual assault.)

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



## What is sexual harassment?

[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 Schools and Colleges (DfE 2021). We ensure that they receive appropriate specialist training, commensurate with their role and that ongoing training is provided for all school staff.

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

## Staff

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

## Governors

We ensure that our trust board/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 trustees/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 trust board/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. Trustees/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. This can be done via:

- [online reporting tool](#),
- [links to national or local organisations](#)
- [list any other systems here](#)

## 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 (e.g., using the [ProjectEVOLVE](#) resources)
- Computing
- PSHE

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.

- [NSPCC training](#)
- Whole staff training
- DSL training

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

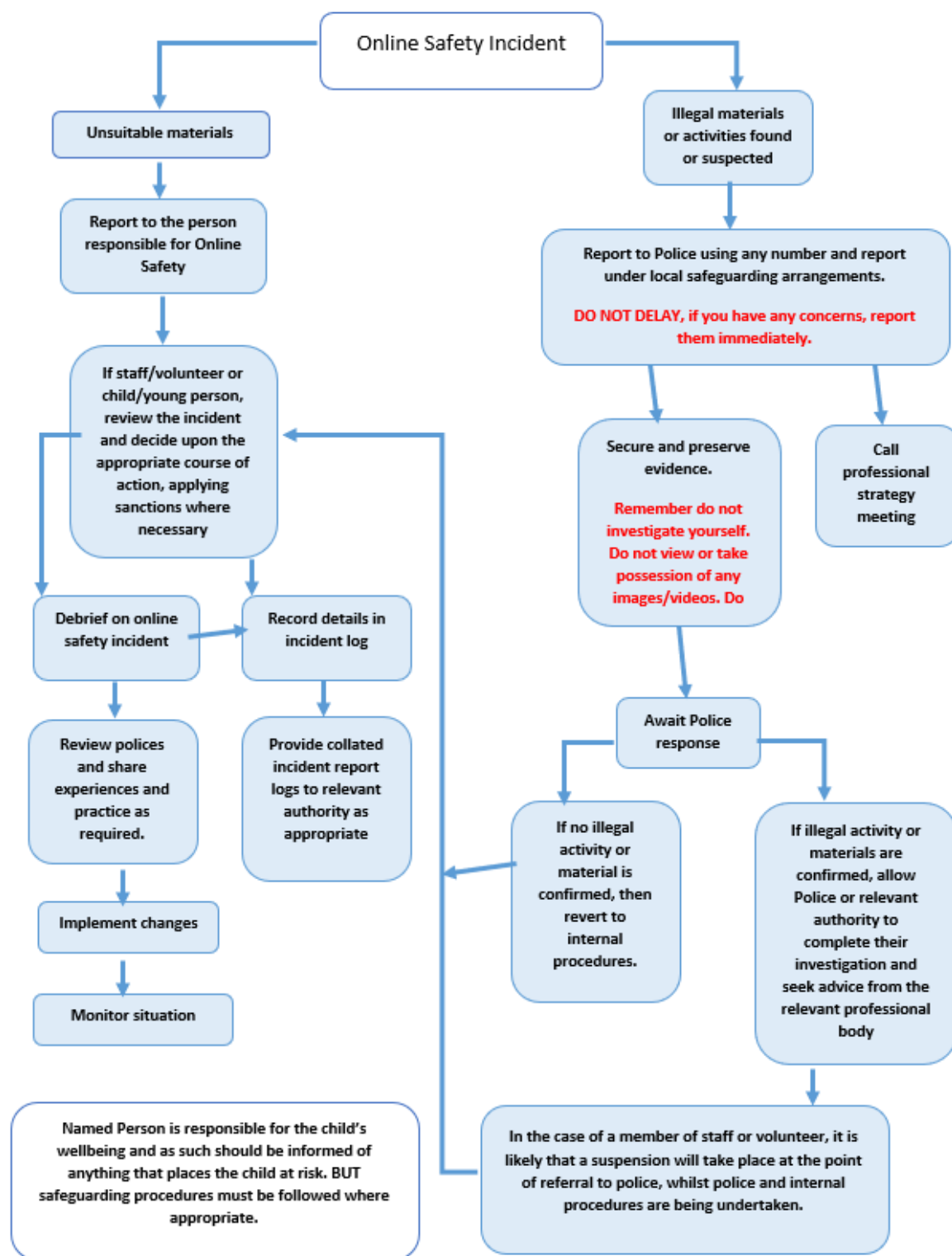
[Lucy Faithful Foundation](#)

[Marie Collins Foundation](#)

[NSPCC National Clinical and Assessment Service \(NCATS\)](#)

[Project deSHAME](#) from [Childnet](#) provides useful research, advice and resources regarding online sexual harassment.

## Responding to incidents of misuse – flow chart



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

Group: .....

Date: .....

Reason for investigation: .....

.....

.....

### Details of first reviewing person

Name: .....

Position: .....

Signature: .....

### Details of second reviewing person

Name: .....

Position: .....

Signature: .....

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

.....

.....

Web site(s) address/device	Reason for concern

### Conclusion and Action proposed or taken




# Reporting Log

Group: .....

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

## Training Needs Audit Log

Group: .....

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

# School Technical Security Policy (including filtering and passwords)

Suggestions for use

## 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 Brent Wallhead (ICT Technician)

## 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**
- Louise Shaw 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
- *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.
- 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 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.

Further guidance can be found from the [National Cyber Security Centre](#) and [SWGfL "Why password security is 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 Louise Shaw – Assistant Headteacher 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**
- The school may wish to recommend to staff and learners (depending on age) that they make use of a 'password vault' these can store passwords in an encrypted manner and can generate very difficult to crack passwords. There may be a charge for these services.
- Passwords should not be set to expire as long as they comply with the above, but should be unique to each service the user logs into.

#### Learner passwords:

- **Records of learner usernames and passwords for foundation phase & key stage one 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 phase should 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.
- 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 [Louise Shaw \(Assistant Headteacher\)](#) Good practice is that the password generated by this change process should be system generated and only known to the user. This password should be temporary and the user should be forced to change their password on first login. The generated passwords should also be long and random.*
- *Where automatically generated passwords are not possible, then a good password generator should be used by [Louise Shaw \(Assistant Headteacher\)](#) 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 Louise Shaw 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.**
- **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/college’s password policy:

- in lessons
- through the acceptable use agreement

#### Audit/Monitoring/Reporting/Review:

The responsible person – [Assistant Headteacher](#) 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 [Assistant Headteacher](#). 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 ([schools should choose their relevant responses](#)):

- **be logged in change control logs**
- **be reported to a second responsible person** ([Headteacher](#)):

All users have a responsibility to report immediately to Assistant Headteacher 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.

- *The school has provided enhanced/differentiated user-level filtering through the use of the [Proxy setting and Netsweeper](#) filtering programme.*
- *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.*
- *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.

### Changes to the Filtering System

No changes are able to be made.

### 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.

### Audit/Reporting

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

- the second responsible person
- 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.

### Further Guidance

[Schools may wish to seek further guidance. The following is recommended:](#)

Schools in England (and Wales) are required *"to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering"* ([Revised Prevent Duty Guidance: for England and Wales, 2015](#)).

The Department for Education '[Keeping Children Safe in Education](#)' requires schools to: *"ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able*



*to access harmful or inappropriate material from the school or colleges IT system” however, schools will need to “be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.”*

In response UKSIC produced guidance on – information on [“Appropriate Filtering”](#)

[Somerset Guidance for schools – questions for technical support](#) – this checklist is particularly useful where a schools uses external providers for its technical support/security.

SWGfL provides a site for schools to test their filtering to ensure that illegal materials cannot be accessed: [SWGfL Test Filtering](#)

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

**The DfE guidance – Searching, Screening and Confiscation was updated in July 2022.**

**Please note this guidance pertains only to schools in England.**

### Introduction

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

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

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

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

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

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

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

The Headteacher must publicise the school behaviour policy, in writing, to staff, parents/carers and learners at least once a year. (There should therefore be clear links between the search etc. policy and the behaviour policy).

DfE advice on these sections of the Education Act 2011 can be found in the document: “Screening, searching and confiscation – Advice for schools” (**updated July 2022**)

It is recommended that Headteachers (and, at the least, one other senior leader) should be familiar with this guidance.

**The DfE Guidance – “Behaviour in Schools” was updated in July 2022 and refers to behaviour online:**

“The way in which pupils relate to one another online can have a significant impact on the culture at school. Negative interactions online can damage the school’s culture and can lead to school feeling like an unsafe place. Behaviour issues online can be very difficult to manage given issues of anonymity, and online incidents occur both on and off the school premises. Schools should be clear that even though the online space differs in many ways, the same standards of behaviour are expected online as apply offline, and that everyone should be treated with kindness, respect and dignity.

Inappropriate online behaviour including bullying, the use of inappropriate language, the soliciting and sharing of nude or semi-nude images and videos and sexual harassment should be addressed in accordance with the same principles as offline behaviour, including following the child protection policy and speaking to the designated safeguarding lead (or deputy) when an incident raises a safeguarding concern.

Many online behaviour incidents amongst young people occur outside the school day and off the school premises. Parents are responsible for this behaviour. However, often incidents that occur online will affect the school culture. Schools should have the confidence to sanction pupils when their behaviour online poses a threat or causes harm to another pupil, and/or could have repercussions for the orderly running of the school, when the pupil is identifiable as a member of the school or if the behaviour could adversely affect the reputation of the school.

Headteachers should decide if **mobile phones** can be used during the school day. Many pupils, especially as they get older, will have one of their own. Allowing access to mobiles in school introduces complexity and risks, including distraction, disruption,

bullying and abuse, and can be a detriment to learning. Headteachers should consider restricting or prohibiting mobile phones to reduce these risks.

If headteachers decide not to impose any restrictions on mobile phones, they should have a clear plan to mitigate the risks of allowing access to phones. This plan, as part of the school's behaviour policy, should outline the approach to mobile phones and be reiterated to all pupils, staff and parents throughout the school year. Headteachers should ensure it is consistently and fairly applied."

**A new Keeping Children Safe in Education guidance document is in force from September 2022.** Schools should be aware of new guidance concerning **Harmful Sexual Behaviour** (see policy template in these appendices):

"Following any report of child-on-child sexual violence or sexual harassment offline or online, schools should follow the general safeguarding principles set out in Keeping children safe in education (KCSIE) - especially Part 5. The designated safeguarding lead (or deputy) is the most appropriate person to advise on the school's initial response. Each incident should be considered on a case-by-case basis.

Schools should be clear in every aspect of their culture that sexual violence and sexual harassment are never acceptable, will not be tolerated and that pupils whose behaviour falls below expectations will be sanctioned. Schools should make clear to all staff the importance of challenging all inappropriate language and behaviour between pupils. Schools should refer to the Respectful School Communities toolkit for advice on creating a culture in which sexual harassment of all kinds is treated as unacceptable."

**Relevant legislation:**

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011 Part 2 (Discipline)
- The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990

This is not a full list of Acts involved in the formation of this advice. Further information about relevant legislation can be found via the above link to the DfE advice document.

## Responsibilities

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

This policy has been written by and will be reviewed by: [Senior Leadership Team](#)

The Headteacher has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data/files on those devices: [Louise Shaw](#)

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

[Members of staff cannot be required to carry out such searches. They can each choose whether or not they wish to be an authorised member of staff.](#)

## Training/Awareness

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

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

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

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

## Policy Statements

### Screening

[DfE "Screening, searching and confiscation – Advice for schools"](#) allows schools to use screening:

["Screening can help provide reassurance to pupils, staff and parents that the school is taking measures to create a calm, safe and supportive environment.](#)

Schools' statutory power to make rules on pupil behaviour and their duties as employers in relation to the safety of staff, pupils and visitors enables them to impose a requirement that pupils undergo screening.

Screening is the use of a walk-through or hand-held metal detector (arch or wand) to scan all pupils for weapons before they enter the school premises..

If a headteacher decides to introduce a screening arrangement, they should inform pupils and parents in advance to explain what the screening will involve and why it will be introduced."

The school should add here details of any screening arrangements that are in place:

Search:

The school **Behaviour Policy** refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data/files on those devices.

The school will already have a policy relating to whether or not mobile phones and other electronic devices are banned, or are allowed only within certain conditions. The school should therefore consider including one of the following statements in the policy:

*Learners are not allowed to bring mobile phones or other personal electronic devices to use in the school.*

If learners breach these rules:

*The sanctions for breaking these rules can be found in the [behaviour policy](#).*

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

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

In carrying out the search:

The authorised member of staff must have reasonable grounds for suspecting that a *learner* is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for. (Whether there are 'reasonable grounds' is a matter decided on by reference to the circumstances witnessed by, or reported to, someone who is authorised and who exercises properly informed professional judgment and has received appropriate training).

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone/personal electronic device before carrying out a search. (The powers included in the Education Act do not extend to devices owned (or mislaid) by other parties e.g. a visiting parent or contractor, only to devices in the possession of learners.)

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

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

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

Extent of the search:

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

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

'Possessions' means any goods over which the learner has or appears to have control – this includes desks, lockers and bags. (schools will need to take account of their normal policies regarding religious garments/headwear and may wish to refer to it in this policy)

A learner's possessions can only be searched in the presence of the learner and another member of staff, except where there is a risk that serious harm will be caused to a person if



the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

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

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

## Electronic devices

The DfE guidance – [Searching, Screening and Confiscation](#) received significant updates in July 2022 and now states:

- Electronic devices, including mobile phones, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, indecent images of children, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour.
- As with all prohibited items, staff should first consider the appropriate safeguarding response if they find images, data or files on an electronic device that they reasonably suspect are likely to put a person at risk
- Staff may examine any data or files on an electronic device they have confiscated as a result of a search, if there is good reason to do so (defined earlier in the guidance as)
  - poses a risk to staff or pupils;
  - is prohibited, or identified in the school rules for which a search can be made or
  - is evidence in relation to an offence.
- If the member of staff conducting the search suspects they may find an indecent image of a child (sometimes known as nude or semi-nude images), the member of staff should never intentionally view the image, and must never copy, print, share, store or save such images. When an incident might involve an indecent image of a child and/or video, the member of staff should confiscate the device, avoid looking at the device and refer the incident to the designated safeguarding lead (or deputy) as the most appropriate person to advise on the school's response. Handling such reports or concerns can be especially complicated and schools should follow the principles as set out in [Keeping children safe in education](#). The UK Council for Internet Safety also provides the following guidance to support school staff and designated safeguarding leads: [Sharing nudes and semi-nudes: advice for education settings working with children and young people](#).

- If a member of staff finds any image, data or file that they suspect might constitute a specified offence, then they must be delivered to the police as soon as is reasonably practicable.
- In exceptional circumstances members of staff may dispose of the image or data if there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files, the member of staff must have regard to the following guidance issued by the Secretary of State
  - In determining whether there is a 'good reason' to examine the data or files, the member of staff should reasonably suspect that the data or file on the device has been, or could be used, to cause harm, undermine the safe environment of the school and disrupt teaching, or be used to commit an offence.
  - In determining whether there is a 'good reason' to erase any data or files from the device, the member of staff should consider whether the material found may constitute evidence relating to a suspected offence. In those instances, the data or files should not be deleted, and the device must be handed to the police as soon as it is reasonably practicable. If the data or files are not suspected to be evidence in relation to an offence, a member of staff may delete the data or files if the continued existence of the data or file is likely to continue to cause harm to any person and the pupil and/or the parent refuses to delete the data or files themselves

The examination of the data/files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge. It is important that authorised staff should have training and sufficient knowledge of electronic devices and data storage.

Members of staff may require support in judging whether the material is inappropriate or illegal. One or more Senior Leaders should receive additional training to assist with these decisions. Care should be taken not to delete material that might be required in a potential criminal investigation.

The school should also consider their duty of care responsibility in relation to those staff who may access disturbing images or other inappropriate material whilst undertaking a search. Seeing such material can be most upsetting. There should be arrangements in place to support such staff. The school may wish to add further detail about these arrangements.

Further guidance on reporting the incident to the police and the preservation of evidence can be found in the SWGfL flow chart in the main School Template Policies document. Local

authorities/local safeguarding partnerships may also have further guidance, specific to their area.

A record should be kept of the reasons for the deletion of data/files. (DfE guidance states and other legal advice recommends that there is no legal reason to do this, best practice suggests that the school can refer to relevant documentation created at the time of any search or data deletion in the event of a learner, parental or other interested party complaint or legal challenge. Records will also help the school to review online safety incidents, learn from what has happened and adapt and report on application of policies as necessary).

### Care of Confiscated Devices

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage/loss of such devices (particularly given the possible high value of some of these devices).

### Audit/Monitoring/Reporting/Review

The responsible person – Assistant Headteacher will ensure that full records are kept of incidents involving the searching for and of electronic devices and the deletion of data/files.

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

The school is required to publish its Behaviour Policy to parents annually (including on its website) – the Behaviour Policy should be cross referenced with this policy on search and deletion. DfE guidance can be found at: <https://www.gov.uk/government/publications/searching-screening-and-confiscation>

## Mobile Technologies Policy (inc. BYOD/BYOT)

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

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

### Potential Benefits of Mobile Technologies

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

### Considerations

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

Schools may consider implementing the use of mobile technologies as a means of reducing expenditure on school provided devices. However, it is important to remember that the increased network management costs and overheads involved in implementing this properly are likely to counterbalance or outweigh any savings.

The use of mobile technologies brings both real benefits and challenges for the whole school community – including teachers - and the only effective way for a school to implement these

successfully is to involve the whole school community from the outset. Before the school embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

A range of mobile technology implementations is possible. The school should consider the following statements and remove those that do not apply to their planned implementation approach.

- The school acceptable use agreements for staff, learners and parents/carers will consider the use of mobile technologies
- The school allows:

	School/devices		Personal devices			
	School owned and allocated to a single user	School owned for use by multiple users	Authorised device <sup>6</sup>	Learner owned	Staff owned	Visitor owned
Allowed in school	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	No	Yes	Yes
Full network access	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	No	No	No
Internet only				No	No	No
No network access				No	Yes	Yes

- **The school has provided technical solutions for the safe use of mobile technology for school devices/personal devices (delete/amend as appropriate):**
  - **All school devices are controlled through the use of Mobile Device Management software**
  - **Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g Internet only access, network access allowed, shared folder network access)**

<sup>6</sup> 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

- **The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices**
- **For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted**
- **Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user.** *These may include; revoking the link between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licenced software etc.*
- *All school devices are subject to routine monitoring*
- *Pro-active monitoring has been implemented to monitor activity*
- **When personal devices are permitted:**
  - *All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access*
  - *Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school*
  - *The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)*
  - *The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues*
  - *The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security*
  - *The school is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues*
- **Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition;**
  - **Devices may not be used in tests or exams**
  - **Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements**

- **Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network**
- **Users are responsible for charging their own devices and for protecting and looking after their devices while in the school**
- **Personal devices should be charged before being brought to the school as the charging of personal devices is not permitted during the school day**
- **Devices must be in silent mode on the school site and on school buses**
- **School devices are provided to support learning. It is expected that learners will bring devices to the school as required.**
- **Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.**
- **The changing of settings (exceptions include personal settings such as font size, brightness, etc...) that would stop the device working as it was originally set up and intended to work is not permitted**
- **The software/apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps**
- **The school will ensure that devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to learners on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.**
- **Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.**
- **Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately**
- *Devices may be used in lessons in accordance with teacher direction*
- *Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances*
- *Printing from personal devices will not be possible*

## Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

### UK Safer Internet Centre

Safer Internet Centre – <https://www.saferinternet.org.uk/>

South West Grid for Learning - <https://swgfl.org.uk/products-services/online-safety/>

Childnet – <http://www.childnet-int.org/>

Professionals Online Safety Helpline - <http://www.saferinternet.org.uk/about/helpline>

Revenge Porn Helpline - <https://revengepornhelpline.org.uk/>

Internet Watch Foundation - <https://www.iwf.org.uk/>

Report Harmful Content - <https://reportharmfulcontent.com/>

[Harmful Sexual Support Service](#)

### CEOP

CEOP - <http://ceop.police.uk/>

ThinkUKnow - <https://www.thinkuknow.co.uk/>

### Others

LGfL – [Online Safety Resources](#)

Kent – [Online Safety Resources page](#)

INSAFE/Better Internet for Kids - <https://www.betterinternetforkids.eu/>

UK Council for Internet Safety (UKCIS) - <https://www.gov.uk/government/organisations/uk-council-for-internet-safety>

### Tools for Schools / other organisations

Online Safety BOOST – <https://boost.swgfl.org.uk/>

360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>

360Data – online data protection self-review tool: [www.360data.org.uk](http://www.360data.org.uk)

SWGfL Test filtering - <http://testfiltering.com/>

UKCIS Digital Resilience Framework - <https://www.gov.uk/government/publications/digital-resilience-framework>

[SWGfL 360 Groups – online safety self review tool for organisations working with children](#)

[SWGfL 360 Early Years – online safety self review tool for early years organisations](#)

### Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - <http://enable.eun.org/>



SELMA – Hacking Hate - <https://selma.swgfl.co.uk>

Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>

Scottish Government - Better relationships, better learning, better behaviour -  
<http://www.scotland.gov.uk/Publications/2013/03/7388>

DfE - Cyberbullying guidance -

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/374850/Cyberbullying  
g Advice for Headteachers and School Staff 121114.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_guidance_for_Headteachers_and_School_Staff_121114.pdf)

Childnet – Cyberbullying guidance and practical PSHE toolkit:

<http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit>

[Childnet – Project deSHAME – Online Sexual Harrassment](#)

[UKSIC – Sexting Resources](#)

Anti-Bullying Network – <http://www.antibullying.net/cyberbullying1.htm>

[Ditch the Label – Online Bullying Charity](#)

[Diana Award – Anti-Bullying Campaign](#)

## Social Networking

Digizen – [Social Networking](#)

UKSIC - [Safety Features on Social Networks](#)

[Children’s Commissioner, TES and Schillings – Young peoples’ rights on social media](#)

## Curriculum

SWGfL Evolve - <https://projectevolve.co.uk>

[UKCCIS – Education for a connected world framework](#)

Department for Education: Teaching Online Safety in Schools

Teach Today – [www.teachtoday.eu/](http://www.teachtoday.eu/)

Insafe - [Education Resources](#)

## Data Protection

[360data - free questionnaire and data protection self review tool](#)

[ICO Guides for Organisations](#)

[IRMS - Records Management Toolkit for Schools](#)

[ICO Guidance on taking photos in schools](#)

## Professional Standards/Staff Training

[DfE – Keeping Children Safe in Education](#)

DfE - [Safer Working Practice for Adults who Work with Children and Young People](#)

[Childnet – School Pack for Online Safety Awareness](#)

[UK Safer Internet Centre Professionals Online Safety Helpline](#)

## Infrastructure/Technical Support/Cyber-security

[UKSIC – Appropriate Filtering and Monitoring](#)

[SWGfL Safety & Security Resources](#)

Somerset - [Questions for Technical Support](#)

SWGfL - [Cyber Security in Schools](#).

NCA – [Guide to the Computer Misuse Act](#)

NEN – [Advice and Guidance Notes](#)

## Working with parents and carers

[SWGfL – Online Safety Guidance for Parents & Carers](#)

[Vodafone Digital Parents Magazine](#)

[Childnet Webpages for Parents & Carers](#)

[Get Safe Online - resources for parents](#)

[Teach Today - resources for parents workshops/education](#)

[Internet Matters](#)

## Prevent

[Prevent Duty Guidance](#)

[Prevent for schools – teaching resources](#)

Childnet – [Trust Me](#)

## Research

[Ofcom –Media Literacy Research](#)

Ofsted: Review of sexual abuse in schools and colleges

Further links can be found at the end of the UKCIS [Education for a Connected World Framework](#)

## Glossary of Terms

<b>AUP/AUA</b>	Acceptable Use Policy/Agreement – see templates earlier in this document
<b>CEOP</b>	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.
<b>CPD</b>	Continuous Professional Development
<b>FOSI</b>	Family Online Safety Institute
<b>ICO</b>	Information Commissioners Office
<b>ICT</b>	Information and Communications Technology
<b>INSET</b>	In Service Education and Training
<b>IP address</b>	The label that identifies each computer to other computers using the IP (internet protocol)
<b>ISP</b>	Internet Service Provider
<b>ISPA</b>	Internet Service Providers' Association
<b>IWF</b>	Internet Watch Foundation
<b>LA</b>	Local Authority
<b>LAN</b>	Local Area Network
<b>MAT</b>	Multi Academy Trust
<b>MIS</b>	Management Information System
<b>NEN</b>	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
<b>Ofcom</b>	Office of Communications (Independent communications sector regulator)
<b>SWGfL</b>	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
<b>TUK</b>	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

A more comprehensive glossary can be found at the end of the UKCIS [Education for a Connected World Framework](#)

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in September 2022. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.