STOKENCHURCH PRIMARY SCHOOL & NURSERY

AIMING HIGH ... FLYING HIGHER

Everything we do makes a difference to our children; empowering minds and shaping futures.

ONLINE SAFETY POLICY

Updated by	Mrs Amy Whelan
Updated when	January 2026
Ratified by	FGB
Ratified when	Spring 2026
Signed by	Dr Gary Murton
Next Review Date	Spring 2027
Statutory Policy	Yes
On school website	Yes

Contents

Introduction

The requirement that Pupils 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. Stokenchurch Primary School and Nursery's Online Safety Policy meets the statutory obligations to ensure that Pupils are safe and are protected from potential harm, both on and off-site.

The DfE Keeping Children Safe in Education statutory guidance requires Local Authorities, Multi Academy Trusts, and schools in England to ensure Pupils 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.*

The DfE Keeping Children Safe in Education guidance suggests that:

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

content*: being exposed to illegal, inappropriate, or harmful content, for example: AI-generated harmful content, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.*

contact*: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.*

conduct*: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and*

commerce*: risks such as online gambling, inappropriate advertising, phishing and or financial scams*

Scope of the Online Safety Policy

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

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

STOKENCHURCH 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:

- headteacher/senior leaders
- Designated Safeguarding Lead (DSL)
- Computing Lead / IT Manager
- staff – including teachers/support staff/technical staff
- governors
- parents and carers
- community users

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for development, monitoring and review

The implementation of this Online Safety Policy will be monitored by: SLT and IT Manager.

The governing body will receive an annual report from the Online Safety Lead on the implementation of the Online Safety Policy (which will include anonymous details of online safety incidents).

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.
Should serious online safety incidents take place, the following external persons/agencies should be informed by the DSL:

Local Authority Designated Officer (LADO) The Buckinghamshire Local Authority Designated Officer (LADO) is responsible for overseeing the management of all allegations against people in a position of trust who work with children in Buckinghamshire on either a paid or voluntary basis.	01296 382070 Secure-lado@buckinghamshire.gov.uk
Thames Valley Police	101 (999 in case of emergency)

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Filtering and monitoring logs
- Internal monitoring data for network activity
- Surveys/questionnaires of:
  - Pupils
  - 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 and groups within the school.

Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the DSL, as defined in Keeping Children Safe in Education.
- 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.
- The headteacher/senior leaders are responsible for ensuring that the DSL / IT Manager / IT support, 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 DSL.
- The headteacher/senior leaders will work with the responsible Governor, the DSL and IT service providers in all aspects of filtering and monitoring.

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"

"Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)"

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

This review will be carried out by the Safeguarding governor, James Baker, who will receive regular information about online safety incidents and monitoring reports. This role includes:

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

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

Designated Safety Lead (DSL)

Keeping Children Safe in Education states that:

"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description."

They (the DSL) "are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college"

They (the DSL) "can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online"

The DSL will:

- Hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- Meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- Attend relevant governing body meetings/groups
- Report regularly to headteacher/senior leadership team
- Be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- Liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)
- Lead the Online Safety Group
- Receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- Have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- Liaise with Computing / PSHE lead to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- Provide (or identify sources of) training and advice for staff/governors/parents/carers/Pupils
- Liaise with (school/local authority/external provider) technical staff, pastoral staff and support staff (as relevant)
- Receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by pupils) with regard to the areas defined In Keeping Children Safe in Education:
    - Content
    - Contact
    - Conduct
    - Commerce

Computing Leads

Computing Leads will work with the DSL to develop a planned and coordinated online safety education programme. This will be provided through:

- A discrete programme using Project EVOLVE
- Links within PHSE and SRE programmes
- Assemblies
- Through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and support staff

School staff are responsible for ensuring that:

- They have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- They understand that online safety is a core part of safeguarding
- They have read, understood, and signed the staff acceptable use agreement (AUA)
- They immediately report any suspected misuse or problem to the DSL for investigation/action, in line with the school safeguarding procedures
- All digital communications with pupils and parents/carers are on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Ensure pupils understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- They supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- In lessons where internet use is pre-planned pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies (n.b. the guidance contained in the SWGfL Safe Remote Learning Resource
- There is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media
- Staff must follow the school's AI Policy regarding the use of Generative AI, ensuring they do not input personal data of pupils into AI tools and that they critically evaluate AI-generated content for bias or inaccuracies

IT Provider

The DfE Filtering and Monitoring Standards says:

"Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider."

"Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support."

"The IT service provider should have technical responsibility for:
- *Maintaining filtering and monitoring systems*
- *Providing filtering and monitoring reports*
- *Completing actions following concerns or checks to systems"*

"The IT service provider should work with the senior leadership team and DSL to:
- *Procure systems*
- *Identify risk*
- *Carry out reviews*
- *Carry out checks"*

"We are aware that there may not be full-time staff for each of these roles and responsibility may lie as part of a wider role within the school, college, or trust. However, it must be clear who is responsible, and it must be possible to make prompt changes to your provision."

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 IT Provider (Turn It On) is responsible for ensuring that:
- They are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- The school technical infrastructure is secure and is not open to misuse or malicious attack
- The school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority / 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 DSL 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 (see appendix 'Technical Security Policy template' for good practice)
- Monitoring systems are implemented and regularly updated as agreed in school policies

Pupils

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

Parents and carers

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 Pupils' acceptable use agreement (agreed by the parent and child upon admission to STOKENCHURCH)
- Publishing information about appropriate use of social media relating to posts concerning the school.
- Seeking their permissions concerning digital images, cloud services etc (via Applicaa)
- 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 Pupils in school.
- The safe and responsible use of their children's personal devices in the school (where this is allowed)

Community users

Community users who access school systems/website/learning platform as part of the wider school provision will be expected to agree to a community user AUA before being provided with access to school systems e.g. Guest Wifi. The school encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to senior leaders and the governing body.
The Online Safety Group could consist of the following members:

- DSL
- Computing Lead
- IT Manager
- SLT
- Online safety governor
- Turn It On IT consultant
- Teacher and support staff members
- Pupils
- Parents/carers

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

- The production/review/monitoring of the school Online Safety Policy/documents
- The production/review/monitoring of the school filtering policy and requests for filtering changes
- Mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- Reviewing network/filtering/monitoring/incident logs, where possible
- Encouraging the contribution of Pupils 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 Pupils in the digital world
- describes how the school will help prepare pupils 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
- is published on the school website.

Acceptable use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

Acceptable use agreements

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

- admission process
- staff induction and handbook
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering See guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) Serious or repeat offences will be reported to the police. The National Crime Agency has a remit to prevent Pupils becoming involved in cyber-crime and harness their activity in positive ways– further information here					X
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)				X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
	Misuse of AI				X	

User actions	Staff and other adults				Pupils			
	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			
Social media			X		X			
Messaging/chat			X		X			
Entertainment streaming e.g. Netflix, Disney+			X		X			
Use of video broadcasting, e.g. YouTube, Twitch, TikTok				X	X			
Sept 2026: Smartphones may be brought to school for travel – Y6 only		X						X
Sept 2026: Non-smartphones may be brought to school for travel – Y5 only								
Sept 2027: Smartphones may be brought into school					X			
Sept 2027: Non-smartphones may be brought to school for travel (Y5 & Y6 only)								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/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
Use of AI within school (as per AI policy)		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 Pupils 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 member of SLT, 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 Pupils

Reporting and responding

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 and other responsible staff have appropriate skills and training to deal with online safety risks
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures, this may include
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy
- Any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority
- Where there is no suspected illegal activity, devices may be checked using the following procedures:
    - One or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported
    - Conduct the procedure using a designated device that will not be used by Pupils 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 using CPOMS
- 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
    - Pupils, through assemblies/lessons
    - Parents/carers, through newsletters, school social media, website

- Governors, through regular safeguarding updates
- Local authority/external agencies, as relevant

The school will make the flowchart in the appendix 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:

Responding to Pupil Actions

Incidents	Refer to class teacher	Refer to SLT	Refer to Headteacher	Refer to Police/Social Work	Inform parents/carers	Remove device/ network/internet access rights	Issue a warning	Inform Computing Lead / IT Manager for relevant action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X	X	X	X			X
Attempting to access or accessing the school network, using another user's account (staff or Pupil) 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	X
Unauthorised downloading or uploading of files or use of file sharing.	X	X						X
Using proxy sites or other means to subvert the school's filtering system.			X		X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident.	X		X		X			X
Deliberately accessing or trying to access offensive or pornographic material.			X	X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.		X			X		X	X
Unauthorised use of digital devices (including taking images)	X	X			X		X	X
Unauthorised use of online services	X	X						X
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.			X		X		X	X
Continued infringements of the above, following previous warnings or sanctions.			X			X		X

Responding to Staff Actions

Incidents	Refer to line manager	Refer to Headteacher	Refer to local authority	Refer to Police	Issue a warning	Disciplinary action	Inform Computing Lead / IT Manager for relevant action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		X	X	X		X	X
Deliberate actions to breach data protection or network security rules.		X	X		X	X	X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X	X		X	X
Using proxy sites or other means to subvert the school's filtering system.	X	X				X	X
Unauthorised downloading or uploading of files or file sharing	X	X				X	X
Breaching copyright or licensing regulations.	X	X				X	X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	X					X	X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		X			X	X	
Using personal e-mail/social networking/messaging to carry out digital communications with Pupils and parents/carers	X	X			X	X	X
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail	X	X			X	X	X
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	X					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 Pupils to take a responsible approach. The education of Pupils in online safety is therefore an essential part of the school's online safety provision. Pupils need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

Keeping Children Safe in Education states:

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

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

- A planned online safety curriculum for all year groups matched against a nationally agreed framework e.g. Education for a Connected Work Framework by UKCIS/DCMS and the SWGfL Project Evolve and regularly taught in a variety of contexts
- Lessons are matched to need; are age-related and build upon prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Pupil 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
- AI literacy is integrated into the curriculum to help pupils understand how Generative AI works, its limitations, and the risks of misinformation, 'deepfakes', and algorithmic bias, in line with the school's AI Policy
- 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 Pupils at different ages and abilities such as those with additional learning needs or those with English as an additional language
- Vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990
- 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 pupils 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 Pupils are allowed to freely search the internet, staff should be vigilant in supervising the Pupils 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 (e.g. addressing emerging technologies such as Generative AI) to ensure the quality of learning and outcomes

Contribution of Pupils

The school acknowledges, learns from, and uses the skills and knowledge of Pupils 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 Pupil feedback and opinion e.g. Pupil Voice surveys
- Appointment of Digital Leaders
- The Online Safety Group has Pupil representation
- Pupils contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger Pupils, online safety campaigns

- Contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.

Staff/volunteers

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 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 / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- The Designated Safeguarding Lead/Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required

Governors

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

- Attendance at training provided by the local authority/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. This will include:

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

Families

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.
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
- Opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc
- The Pupils – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by Pupils leading sessions at parent/carer evenings
- Letters, newsletters, website, learning platform
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers (see Links to other organisations or documents at end of this document)
- Sharing good practice with other schools in clusters and or the local authority

Technology

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school 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 & Monitoring

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

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

Filtering

- The school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering
- Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- There is a clear process in place to deal with, and log, requests/approvals for filtering changes (see Appendix 9 for more details)
- Filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different groups of users: staff/pupils, etc.)
- The school has an Electronic Devices (including mobile phones) policy (see Appendix 5) and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice
- Access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice

Monitoring

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

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 informed by the school's risk assessment. These may include:

- Physical monitoring (adult supervision in the classroom)
- Internet use is logged, regularly monitored and reviewed
- Filtering logs are regularly analysed and breaches are reported to senior leaders
- Pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- Where possible, school technical staff regularly monitor and record the activity of users on the school technical systems
- Use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)

Technical Security

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

- Responsibility for technical security resides with SLT who may delegate activities to identified roles.
- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by the SLT/Online Safety Group
- Password policy and procedures are implemented, consistent with guidance from the National Cyber Security Centre

- All users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details
- All school networks and system will be protected by secure passwords
- The administrator passwords for school systems are kept in a secure place, e.g. school safe
- There is a risk-based approach to the allocation of Pupil usernames and passwords. (see 'Technical security policy template' in Appendix 9 for more information)
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling are securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software
- There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud
- The Bursar / IT Manager are 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
- Use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- Staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider
- Removable media is not permitted unless approved by the SLT/IT service provider
- Systems are in place to control and protect personal data and data is encrypted at rest and in transit
- Mobile device security and management procedures are in place
- Guest users are provided with appropriate access to school systems based on an identified risk profile

Mobile technologies

The school acceptable use agreements for staff, pupils and community users outline the expectations around the use of mobile technologies.

The school allows:

	School devices			Personal devices		
	School owned for individual use	School owned for multiple users	Authorised device	Student owned	Staff owned	Visitor owned
Allowed in school	✓	✓	✓	✓ (Y5/6 to be stored away by staff during day)	✓	✓
Full network access	✓	✓	✓	×	×	×
Internet only				×	✓ (Guest Wifi)	✓ (Guest Wifi)
No network access				×		

Social media

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to Pupils 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 pupils, parents/carers

School staff should ensure that:

- No reference should be made in social media to pupils, 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 staff breaks within 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

Digital and video images

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

- The school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies
- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images
- Staff/volunteers must be aware of those pupils 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 pupils in the digital/video images
- Staff are allowed to take digital/video images on school devices 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 pupils are appropriately dressed
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with Online Safety Policy
- Pupils' 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 pupils are taken for use in school or published on the school website/social media

- Parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- Images will be securely stored in line with the school retention policy

Online Publishing

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

- Public-facing website
- Social media
- Online newsletters

The school website is hosted by Juniper Education and managed by the IT Manager. The school ensures that the 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 Pupil work, images or videos are published, their identities are protected, and full names are not published.

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) from Turn It On who has effective understanding of data protection law and is free from any conflict of interest. In addition, there is a Data Protection Lead (DPL) member of 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 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. Procedures are be in place to enable staff to work from home (i.e. VPN access to the school network, or a work laptop provided)
- 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, and secure password protected devices.

The Personal Data Advice and Guidance in the appendix 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, Pupils; 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 Local Authorities to help ensure the development of a consistent and effective local online safety strategy

Appendices

A1 - Pupil Acceptable Use Agreement

This is agreed by parents (to discuss with their children) upon admission to the school. In Upper KS2, children are reminded in lessons of the agreement.

At Stokenchurch Primary School, we understand the importance of children accessing the internet for education and personal development. This includes social media platforms, games and apps. We aim to support children and young people in making use of these in their learning. However, we also recognise that safeguards need to be in place to ensure children are kept safe at all times. This agreement is part of our overarching code of behaviour for children, staff and volunteers. Please read and discuss this agreement with your child and then sign it, ask your child to sign it, and return it to school.

Young person's agreement:

- I will be responsible for my behaviour when using the internet, including social media platforms, games and apps. This includes the resources I access and the language I use
- I will not deliberately browse, download or upload material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to a responsible adult
- I will not send anyone material that could be considered threatening, bullying, offensive or illegal
- I will not give out any personal information online, such as my name, phone number or address
- I will not reveal my passwords to anyone
- I will not arrange a face-to-face meeting with someone I meet online unless I have discussed this with my parents and am accompanied by a trusted adult
- If I am concerned or upset about anything I see on the internet or any messages that I receive, I know I must talk to an adult that I trust
- I understand that my internet use at STOKENCHURCH will be monitored and logged and can be made available to my teacher. I understand that these rules are designed to keep me safe and that if I choose not to follow them, my teacher may contact my parents/carers
- I understand that everything I write on the internet or in a text/WhatsApp message is 'digitally permanent' and could be seen and shared by anyone

A2 - Use of Digital/Video Images for Parents/Carers

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

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

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

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

As the school is collecting personal data by issuing this form, it should inform parents/carers as to:

This form (electronic or printed)	The images
Who will have access to this form	Where the images may be published. Such as; X (formerly known as Twitter), Facebook, the school's website, local press, etc. (see relevant section of form below)
Where this form will be stored	Who will have access to the images
How long this form will be stored for	Where the images will be stored
How this form will be destroyed	How long the images will be stored for
	How the images will be destroyed
	How a request for deletion of the images can be made

Digital/Video Images Permission Form

Upon admission, the following consents are collected from parents/carers:

- I consent to the use of Tapestry (see explanation above)
- I consent to my child's image being used on school displays
- I consent to my child's image being used in local media (local newspapers)
- I consent to my child's image being used on social media platforms
- I consent to the school recording my child (eg. assemblies, school productions and learning journey)
- I consent to my child taking part in Local Visits/Events (within 3 miles)
- I consent to my child taking part in non-residential visits within UK
- I consent to my child's image being used on the school website
- I consent to my child's image being used in the school newsletter
- I consent to my child's image being used in a class group photograph
- I consent to my mobile phone number and e-mail address being used to receive text messages and e-mails from the school via the Parent Mail service
- I consent to my child receiving First Aid from trained staff
- I consent to my child receiving urgent dental/medical/surgical treatment
- I consent to my Child's Medical info may be shared: NHS/health professionals
- I consent to my child having plasters applied
- I consent to the school's ICT Acceptable Use agreement
- I confirm I have discussed the Home School Agreement with my child

A3 - Staff (and Volunteer) Acceptable Use Policy Agreement

Whilst our school promotes the use of technology or devices, and understands the positive effects they can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology and devices appropriately. Any misuse of technology and devices will not be taken lightly and will be reported to the headteacher in order for any necessary further action to be taken. Non-compliance with this policy may result in disciplinary action, including warnings, suspension, or referral to governing bodies. Illegal activity may lead to police involvement.

This agreement outlines staff members' responsibilities when using technology and devices, both school-owned and personal, and applies to all staff, volunteers, contractors and visitors. The school may undertake monitoring activities of employees to ensure the quality and quantity of work. The school will ensure that any monitoring activities undertaken are lawful and fair to workers, as well as meet data protection requirements.

If any monitoring activities are undertaken, then the school will ensure that employees are made aware of the nature, reasons, and extent of the monitoring, that the monitoring has a clearly defined purpose, and that it is as unintrusive as possible to the employees.

Information which is gathered from monitoring activities must have a lawful basis. The school recognises the importance of protecting workers' rights and privacy, especially as remote working becomes more common. Excessive monitoring in remote work environments can negatively impact both data protection rights and the personal lives of employees.

The school will ensure that the monitoring of workers is necessary for the identified reasons. The school will also ensure that all suitable safety checks are carried out prior to monitoring activities. This policy also ensures that staff are protected from risks associated with the misuse of technology, including safeguarding their professional reputation.

Please read this agreement carefully, and sign at the bottom to show you agree to the terms outlined.

Data protection and cyber-security

I will:

- Use technology and devices, including the use and storage of personal data, in line with data protection legislation, including the Data Protection Act 2018 and UK GDPR
- I will ensure that any personal data, whether digital or paper-based, is stored securely and only shared or transferred as outlined in the school's Data Protection Policy
- Ensure that any digital data transferred outside the secure network must be encrypted, and paper-based personal data must be stored in lockable storage

I will not:

- Attempt to bypass any filtering, monitoring and security systems
- Share school-related passwords with pupils, staff, parents or others unless permission has been given for me to do so
- Copy or remove any data from Stokenchurch Primary School at the end of my employment

Using technology in school

I will:

- Follow the Staff ICT and Electronic Devices Policy
- Only use ICT systems which I have been permitted to use
- Ensure I obtain permission prior to accessing materials from unapproved sources
- Only use the internet for personal use during out-of-school hours, including break and lunch time
- Only use recommended removable media and keep this securely stored
- I will immediately report any faults or damage to school equipment, whether accidental or otherwise, to the IT Manager

I will not:

- Install any software onto school ICT systems unless instructed to do so by the headteacher or IT Manager
- Attempt to access, download, or share illegal materials, including but not limited to child sexual abuse images, criminally racist material, or content promoting terrorism or extremism

Emails

I will:

- Only use the approved email accounts that have been provided to me when sending communications regarding school business
- Ensure any personal information that is being sent via email is only sent to the relevant people and is appropriately protected

I will not:

- Use personal emails to send and/or receive school-related personal data or information, including sensitive information
- Use personal email accounts to contact pupils or parents

School-owned devices

I will:

- Only use school-owned devices outside of school as set out in the Online Safety policy
- Only access websites and apps that have been approved by the headteacher
- Understand that the usage of my school-owned devices will be monitored
- Keep my school-owned devices safe e.g. not leaving it on public display
- Transport school-owned devices safely
- Provide suitable care for my school-owned devices at all times
- Only communicate with pupils and parents on school-owned devices using appropriate channels
- Ensure I install and update security software on school-owned devices as directed by the IT Manager
- Seek permission from the headteacher before using a school-owned device to take and store photographs or videos of pupils, parents, staff and visitors
- Immediately report any damage or loss of my school-owned devices to the IT Manager
- Immediately report any security issues, such as downloading a virus, to the IT Manager
- Understand that I am expected to pay an excess for any repair or replacements costs where the device was damaged or lost as a result of my own negligence
- Make arrangements to return school-owned devices to the IT Manager upon the end of my employment at the school

I will not:

- Permit any other individual to use my school-owned devices without my supervision, unless otherwise agreed by the headteacher
- Install any software onto school-owned devices unless instructed to do so by the headteacher or IT Manager
- Use school-owned devices to send inappropriate messages, images, videos or other content
- Use school-owned devices to view, store, download or share any inappropriate, harmful or illegal content
- Use school-owned devices to access personal social media accounts

Personal devices

I will:

- Only use personal devices during out-of-school hours, including break and lunch times
- Ensure personal devices are either switched off or set to silent mode during school hours
- Only make or receive calls in specific areas, e.g. the staff room, empty classroom outside of lesson times
- Store personal devices appropriately during school hours, e.g. a lockable cupboard in the classroom
- Understand that I am liable for any loss, theft or damage to my personal devices

I will not:

- Use personal devices to communicate with pupils or parents
- Access the school's Wi-Fi using a personal device unless permission to do so has been granted by the headteacher or IT Manager
- Use personal devices to take photographs or videos of pupils or staff
- Store any school-related information on personal devices unless permission to do so has been given by the headteacher

Social media and online professionalism

I will:

- Follow the school's Social Media Policy
- Ensure that posts on any online platforms do not compromise my professional responsibilities or the school's reputation

- Ensure I apply necessary privacy settings to social media accounts

I will not:
- Communicate professionally with pupils or parents over personal social media accounts
- Accept 'friend' or 'follow' requests from any pupils or parents over personal social media accounts in my capacity as a staff member
- Post any comments or posts about the school on any social media platforms or other online platforms which may affect the school's reputability
- Post any defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, on any online website
- Post or upload any images and videos of pupils, staff or parents on any online website without consent from the individuals in the images or videos
- Give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels

Working from home

I will:
- Not transfer any personal data from a school-owned device to a personal device
- Ensure my personal device has been assessed for security by the DPO and IT Manager before it is used for home working
- Ensure no unauthorised persons, such as family members or friends, access any personal devices used for home working

Training

I will:
- Participate in any relevant training offered to me, including cyber-security and online safety
- Allow the IT Manager and DPO to undertake regular audits to identify any areas of need I may have in relation to training
- Employ methods of good practice and act as a role model for pupils when using the internet and other digital devices
- Deliver any training to pupils as required

Reporting misuse

I will:
- Report any misuse by pupils or staff members breaching the procedures outlined in this agreement to the headteacher
- Understand that my use of the internet will be monitored by the IT Manager and recognise the consequences if I breach the terms of this agreement
- Understand that the headteacher may decide to take disciplinary action against me, in accordance with the Disciplinary Policy and Procedure, if I breach this agreement

Monitoring workers

I understand that:
- The school will notify employees when monitoring takes place and that the school will clearly explain what personal information of mine is collected and how it's utilised and maintained
- Monitoring is often used for security purposes, managing employees' performance, and monitoring sickness and attendance
- Monitoring technologies include, but are not limited to, camera surveillance, webcams, technologies for timekeeping and keyboard activity, productivity tools, internet activity trackers, body-worn devices, and hidden audio recording
- Personal data relating to myself which is collected from monitoring activities is securely kept and protected and isn't kept for any longer than necessary by the school
- The school will factor in increased expectations of privacy if I work from home
- The school will conduct its monitoring activities in a way that's fair and reasonably expected
- The school will conduct its monitoring activities with transparency, clearly explaining how and why they process my information
- The school will conduct its monitoring activities in a way that's accountable and compliant with UK GDPR
- I can object to having my personal information collected and processed if the lawful basis which the school is relying on is a public task or legitimate interests based on my personal situation

- The school may refuse to comply with the objection if they can demonstrate that the monitoring is for legitimate interests which override my interests, rights, and freedoms, or that the monitoring is for establishment, exercise, or defence of legal claims
- Tools for monitoring workers continue to become increasingly sophisticated, and that the school will inform me if they choose to use solely automated processes for monitoring activities
- I can access the information collected by the school by making a subject access request (SAR)
- The school will carry out a data protection impact assessment (DPIA) prior to undertaking their monitoring activities. Completing a DPIA identifies and minimises any potential risks that come with monitoring activities

Agreement

I certify that I have read and understood this agreement, and ensure that I will abide by each principle.

Name	
Signature	
Date	

A4 - Acceptable Use Agreement for Community Users

This acceptable use agreement is intended to ensure:

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

Community User Acceptable Use Agreement

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

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

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

Name	
Signature	
Date	

A5 - Electronic Devices (including Mobile Phones) Policy

1. INTRODUCTION AND AIMS

At Stokenchurch Primary School, we recognise that mobile phones and electronic devices, including smartphones, tablets, laptops, and smartwatches, are important aspects of daily life for our pupils, parents, staff, and the wider school community. This policy sets out guidelines for the responsible and safe use of both mobile phones and electronic devices, supporting the school's other policies, particularly those related to child protection, behaviour, and data protection.

The aims of this policy are:

- To promote safe and responsible use of mobile phones and electronic devices.
- To provide clear guidelines for mobile phone and electronic device use for pupils, staff, parents, and volunteers.
- To address challenges posed by these devices in school, such as:
  - Risks to child protection
  - Data protection issues
  - Potential disruption to lessons
  - Risks of theft, loss, or damage
  - Ensuring the appropriate use of technology in the classroom
  - Evidence of negative impact of children owning smartphones

2. ROLES AND RESPONSIBILITIES

2.1 Staff

All staff, including teachers, support staff, and supply staff, are responsible for enforcing this policy. Volunteers or other individuals engaged by the school must inform a staff member if they observe any breach of this policy. The headteacher is responsible for reviewing the policy every three years, ensuring its effectiveness, and holding staff and pupils accountable for its implementation.

3. USE OF MOBILE PHONES AND ELECTRONIC DEVICES BY STAFF

3.1 Personal Mobile Phones and Electronic Devices

Staff (including volunteers and contractors) are not permitted to make or receive calls, send texts, or use electronic devices during contact time when children are present. Personal mobile phones and devices should be used only in non-contact time and in areas where pupils are not present, such as the staff room. There may be specific instances where staff need to use their mobile phones or devices during contact time, such as for emergency contact with a child or dependent, or for family emergencies. The headteacher will decide on a case-by-case basis whether special arrangements are necessary. In case of an emergency, staff may use the school office contact number (01494 482112).

3.2 Data Protection

Staff must not use personal mobile phones or electronic devices for processing personal data or any other confidential school information. Further details are outlined in the Data Protection policy.

3.3 Safeguarding

Staff must not share their personal contact details with parents or pupils and must not connect with them through social media or messaging apps. Personal devices should not be used to take photos or recordings of pupils, their work, or anything else that could identify a pupil. If it is necessary to take photos for lessons, school trips, or activities, this must be done using school equipment e.g. staff iPads.

3.4 Use of Personal Devices for Work Purposes

In certain circumstances, staff may need to use personal electronic devices for work, such as:

- Emergency evacuations
- Supervising off-site trips or residential visits
- Staff must adhere to the staff code of conduct, avoid using devices to contact parents (unless via the school office), and refrain from taking photos of pupils.

3.5 Sanctions

Failure to comply with this policy may result in disciplinary action as outlined in the school's staff disciplinary policy.

4. USE OF MOBILE PHONES AND ELECTRONIC DEVICES BY PUPILS

We recognise that mobile phones are part of everyday life for many children and can help them feel secure, particularly when travelling to and from school. However, smartphones in particular can also present significant

distractions, safeguarding concerns, and opportunities for unkind behaviour. In light of this, and based on growing evidence about their impact on wellbeing and learning, we are introducing the following phased restrictions:

- From September 2026, for pupils in Year 6: children may continue to bring a mobile phone (including smartphone) or device into school if necessary for travel to and from school. The device must be labelled, switched off before entering the school gates, and handed to the class teacher at the start of the day and collected at the end of the day. Children must not turn phones on until they have left the school site at the end of the day. The school will not be responsible for lost, damaged, or stolen devices. (The phone must be switched off so that notifications do not get sent to a child's smartwatch even when the phone is locked away)
- From September 2026, for pupils in Year 5: children may bring a basic mobile phone into school, provided it is a non-smartphone (often referred to as a brick phone, dumb phone, or start phone) that can only make calls and send SMS texts. The device must be labelled, switched off before entering the school gates, and handed to the class teacher at the start of the day and collected at the end of the day. Children must not turn phones on until they have left the school site at the end of the day. The school will not be responsible for lost, damaged, or stolen devices.
- From September 2027, smartphones will not be allowed on school grounds for any children. If there are exceptional circumstances that require a child to bring in a smartphone into school each day, for example if it is used as a medical device, parents/carers must request written permission from the headteacher in advance.
- Pupils are not allowed to bring mobile phones or electronic devices on trips

4.1 Sanctions

- Smartphones brought to school without permission will be confiscated under sections 91 and 94 of the Education and Inspections Act 2006) and returned at the end of the day – and must be collected in person by a parent/carer. Repeated breaches may result in further sanctions in line with the school's behaviour policy. Where mobile phones are used in or out of school to bully or intimidate others, then the head teacher does have the power to intervene 'to such an extent as it is reasonable to regulate the behaviour of pupils when they are off the school site' - refer to Anti-Bullying Policy.
- In the event of a pupil's mobile phone being in school, staff have the power to search pupils' phones, as set out in the DfE's guidance on searching, screening and confiscation.

Certain types of conduct, bullying or harassment can be classified as criminal conduct. The school takes such conduct extremely seriously, and will involve the police or other agencies as appropriate.
Such conduct includes, but is not limited to:

- Sexting (consensual and non-consensual sharing nude or semi-nude images or videos)
- Upskirting
- Threats of violence or assault
- Abusive calls, emails, social media posts or texts directed at someone on the basis of someone's ethnicity, religious beliefs or sexual orientation

5. USE OF MOBILE PHONES AND ELECTRONIC DEVICES BY PARENTS, VOLUNTEERS, AND VISITORS

Parents, volunteers, and visitors must comply with this policy while on school premises:

- Mobile phones and electronic devices should not be used to take pictures or recordings of pupils unless it's a public event or of their own child.
- Photos or recordings should only be for personal use and not posted online without consent.
- Phones or devices should not be used during lessons or while working with pupils.

5.1 School Trips and Visits

Parents and volunteers supervising trips or visits must:

- Not use phones or devices to contact other parents
- Not take photos or recordings of pupils or anything that could identify them, unless specifically authorised
- Enforce the school's mobile phone and electronic device policy for pupils on trips

Parents must contact the school office if they need to reach their child during the school day, rather than calling their child's personal phone or device.

6. MONITORING AND REVIEW

The school is committed to ensuring that this policy positively impacts pupils' education, behaviour, and welfare. The policy will be reviewed regularly, taking into account:

- Feedback from parents, pupils, and teachers
- Records of behaviour and safeguarding incidents
- Advice from the Department for Education and other relevant organisations

A6 - Online Safety Group Terms of Reference

1. Purpose

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

2. Membership

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

The composition of the group should include:

- SLT member/s
- Computing Lead
- IT Manager
- Designated Safeguarding Lead (DSL)
- Online Safety Lead (OSL)
- Teaching staff member
- Support staff member
- Governor
- Parent/Carer
- IT Support Provider
- Pupil representation – for advice and feedback

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 members
- Inviting other people to attend meetings when required
- Guiding the meeting according to the agenda and time available
- Ensuring all discussion items end with a decision, action or definite outcome
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. Duration of Meetings

Meetings shall be held termly for a period of 1 hour.

5. Functions

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

- To keep up to date with new developments in the area of online safety
- To (at least) annually review and develop the online safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the online safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching/learning/training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through:
    - Staff meetings
    - Pupil forums (for advice and feedback)
    - Governors meetings
    - Surveys/questionnaires for Pupils, parents/carers and staff

    - Parents evenings
    - Website/newsletters
    - Online safety events
    - Internet Safety Day (annually held on the second Tuesday in February)
    - Other methods
- To ensure that monitoring is carried out of Internet sites used across the schools
- To monitor filtering/change control logs (e.g. requests for blocking/unblocking sites)
- To monitor the safe use of data across the schools
- To monitor incidents involving cyberbullying for staff and Pupils

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 Stokenchurch Primary School & Nursery have been agreed.

Signed by (SLT): Date:
Date for review:

A7 – Computer Misuse and Cyber Choices Policy

All key stakeholders, including the school IT service provider, have responsibility for the safeguarding of young people from computer misuse and are aware of the Cyber Choices programme led by the National Crime Agency (NCA) and managed locally by Regional Organised Crime Units (part of the national policing network). The risks to young people of crossing the line into committing cybercrimes is a safeguarding issue. All staff are made aware of the safeguarding risks of computer misuse.

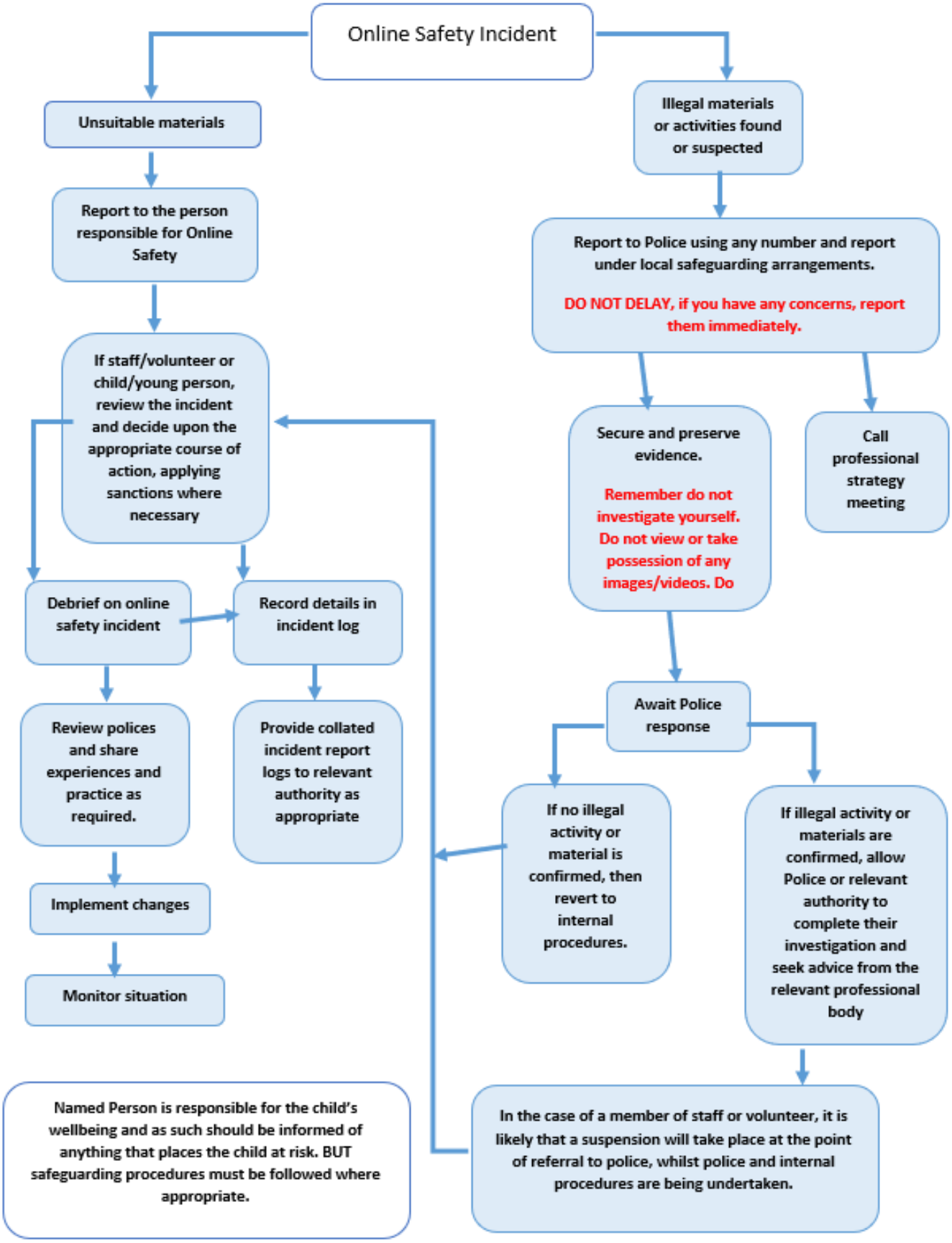
Pupils agree to the Acceptable Use Policy (AUP) which outlines acceptable online behaviours and explains that some online activity is illegal. Acceptable computer use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Any breach of the AUP or activity by a Pupil that may constitute a cybercrime, in school or at home, will be referred to the Designated Safeguarding Lead for consideration as a safeguarding risk.

Where the DSL believes that the Pupil may be at risk of committing cybercrimes, or to already be committing cybercrimes, a referral to the local Cyber Choices programme will be made. Where the DSL is unsure if a Pupil meets the referral criteria, advice should be sought from the local Cyber Choices team.

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

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

A8 – Responding to incidents of misuse – flow chart



A9 - School Technical Security Policy (including filtering, monitoring and passwords)

Introduction

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

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

This template is not designed to reproduce the entirety of the DfE's standards, but is designed to support governors and senior leaders in the production of a technical security policy. Governors and senior leaders remain responsible for the school's technical security.

Responsibilities

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

Policy statements

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

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements (if not managed by the Local Authority/MAT, these may be outlined in Local Authority/other relevant body technical guidance)
- Cyber security is included in the school risk register
- There will be regular reviews and audits of the safety and security of school technical system
- Servers, wireless systems, and cabling must be securely located and physical access restricted
- There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud
- Appropriate security measures (including updates) are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data, including operating systems
- The school's infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc
- Responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff
- All users will have clearly defined access rights to school technical systems and accounts are deleted when the user leaves. Details of the access rights available to groups of users will be recorded by the IT manager/IT service provider and will be reviewed, at least annually, by the online safety group
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- The IT Service Provider, in partnership with Governors/SLT/DSL, regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement
- An appropriate system is in place (CPOMS) for users to report any actual/potential technical incident to the SLT/DSL/Online Safety Lead (OSL)
- The bursar and IT Manager are 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 (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Remote (classroom/network) management tools are used by staff to control workstations and view users' activity
- Guest users are provided with appropriate access to school systems based on an identified risk profile
- School-owned devices should be used outside of school as set out in the Online Safety policy
- By default, users do not have administrator access to any school-owned device
- An agreed policy is in place regarding the use of removable media by users on school devices
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured

Password Security

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

Policy Statements:

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

Pupil passwords:

- For younger children and those with special educational needs, Pupil usernames and passwords can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. Password complexity for these users is reduced and should not include special characters.
- Users will be required to change their password if it is compromised. (Note: passwords should not be regularly changed but should be secure and unique to each account.)
- Pupils will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

Filtering and Monitoring

Introduction to Filtering

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

Your filtering system should be operational, up to date and applied to all:

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

Your filtering system should:

- filter all internet feeds, including any backup connections.

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

Mobile and app content is often presented in a different way to web browser content. If your users access content in this way, you should get confirmation from your provider as to whether they can provide filtering on mobile or app technologies. A technical monitoring system should be applied to devices using mobile or app content to reduce the risk of harm.

Introduction to Monitoring

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

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

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

Filtering and Monitoring Responsibilities

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

Role	Responsibility	Name / Position
Responsible Governor	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.	James Baker / Governor
Senior Leadership	Team member responsible for ensuring these standards are met and: • procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of your provision • overseeing reports Ensure that all staff: • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns	Stephen Sloan / Deputy Head & DSL
Designated Safeguarding Lead	Lead responsibility for safeguarding and online safety, which could include overseeing and acting on: • filtering and monitoring reports • safeguarding concerns • checks to filtering and monitoring systems	Stephen Sloan / Deputy Head & DSL
IT Service Provider	Technical responsibility for: • maintaining filtering and monitoring systems • providing filtering and monitoring reports • completing actions following concerns or checks to systems	Turn It On / IT Consultants
All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:	• they witness or suspect unsuitable material has been accessed • they can access unsuitable material • they are teaching topics which could create unusual activity on the filtering logs	

Role	Responsibility	Name / Position
	• there is failure in the software or abuse of the system • there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks • they notice abbreviations or misspellings that allow access to restricted material	

Policy Statements

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

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

Changes to Filtering and Monitoring Systems

Staff / pupils may request changes to the filtering and monitoring systems. The DSL / OSL will consider the application and request (by email) any necessary changes to be made by Exa who provide the filtering and monitoring system. Exa will also query any request which is flagged as being unusual and requires additional authorisation. The DSL and OSL are the two named members of staff who can authorise changes to the policy.

Filtering and Monitoring Review and Checks

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

Reviewing the filtering and monitoring provision

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

The review will take account of:

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

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

- Related safeguarding or technology policies and procedures
- Roles and responsibilities
- Training of staff
- Curriculum and learning opportunities
- Procurement decisions
- How often and what is checked
- Monitoring strategies

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

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

Checking the filtering and monitoring systems

Checks to filtering and monitoring systems are completed and recorded as part of the filtering and monitoring review process. How often the checks take place will be based on the context, the risks highlighted in the filtering and monitoring review, and any other risk assessments. Checks will be undertaken from both a safeguarding and IT perspective.

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

- School owned devices and services, including those used off site
- Geographical areas across the site
- User groups, for example, staff, pupils and guests

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

- When the checks took place
- Who did the check
- What was tested or checked
- Resulting actions

Training/Awareness:

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

- At induction
- At whole-staff/governor training
- Through the awareness of policy requirements
- Through the acceptable use agreements
- In regular updates throughout the year

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

Pupils are made aware of the expectations of them:

- In lessons (the schools should describe how this will take place)
- Through the acceptable use agreements

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

Audit/Monitoring/Reporting/Review:

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

- Training provided
- User logons
- Security incidents related to this policy
- Annual online safety reviews including filtering and monitoring
- Changes to the filtering system
- Checks on the filtering and monitoring systems

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”. Furthermore, the Department for Education’s statutory guidance ‘Keeping Children Safe in Education’ obliges schools and colleges in England to “ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness” and they “should be doing all that they reasonably can to limit children’s exposure to the above risks from the school’s or college’s 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.” Ofsted concluded as far back as 2010 that “Pupils in the schools that had ‘managed’ systems had better knowledge and understanding of how to stay safe than those in schools with ‘locked down’ systems. Pupils were more vulnerable overall when schools used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves.”

To further support schools and colleges in England, the Department for Education published Digital and Technology standards.

The UK Safer Internet Centre has produced guidance on “Appropriate Filtering and Monitoring” SWGfL, on behalf of UK Safer Internet Centre and DfE, developed further Filtering and Monitoring | SWGfL information for schools and colleges, including a checklist alongside further support for Governors

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

A10 – Privacy Notice (How we use pupil information)

Stokenchurch Primary School are a data controller for the purposes of the UK General Data Protection Regulation. We collect and hold personal information from you about your child and may receive information about your child from their previous school or college, the Local Authority, the Department of Education (DfE) and the Learning Records Service.

The categories of pupil information that we process include:

- Personal identifiers and contacts (such as name, unique pupil number, contact details and address)
- Characteristics (such as ethnicity, language, and free school meal eligibility)
- Safeguarding information (such as court orders and professional involvement)
- Special educational needs (including the needs and ranking)
- Medical and administration (such as doctors information, child health, dental health, allergies, medication and dietary requirements)
- Attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- Assessment and attainment (such as key stage 1 and phonics results, post 16 courses enrolled for and any relevant results)
- Behavioural information (such as exclusions and any relevant alternative provision put in place)
- Trips/activities held securely on Evolve
- Online learning
- Free school meals management

Why we collect and use pupil information

The personal data collected is essential, for the school to fulfil its' official functions and meet legal requirements. We collect and use pupil information, for the following purposes:

a) to support pupil learning, including using various online platforms and tools (specific platforms may change over time)
b) to monitor and report on pupil attainment progress
c) to provide appropriate pastoral care
d) to assess the quality of our services
e) to keep children safe (food allergies, or emergency contact details)
f) to meet the statutory duties placed upon us for DfE data collections
g) to provide wrap around care
h) for Safeguarding and Child Protection including KCSiE 2022 filtering and monitoring

Under the UK General Data Protection Regulation (UK GDPR), the lawful bases we rely on for processing pupil information are:

- Article 6.1.e states that the use of personal data is justified if 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'. In this instance, the requirement for the school to deliver education under the Education Act (1996) requires us to collect information to deliver this service.
- Article 9 covers the use of sensitive personal information (this includes health and social care information). This is justified either by article 9.2.a (consent from the data subject) or article 9.2.e (processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services).

How we collect pupil information

We obtain pupil information via registration forms at the point of admission to school. In addition, when a child joins us from another school, we are sent a secure file containing relevant information.

Pupil data is essential for the schools' operational use. Whilst the majority of pupil information you provide to us is mandatory, some of it requested on a voluntary basis. In order to comply with the data protection legislation, we will inform you at the point of collection, whether you are required to provide certain pupil information to us or if you have a choice in this and we will tell you what you need to do if you do not want to share this information with us.

How we store pupil data

We hold pupil data securely for the set amount of time shown in our data retention schedule. For more information on our data retention schedule and how we keep your data safe, please contact our DPL Judy Pope by email: office@stokenchurchprimary.bucks.sch.uk or telephone 01494 482112

Who we share pupil information with

We routinely share pupil information with:

- Schools that the pupils attend after leaving us
- Our local authority
- Safeguarding agencies
- The Police
- The Department for Education (DfE)
- School governors
- The NHS
- Trip and activity providers
- NFER – provider of Buckinghamshire 11+ test
- Other parties where there is a legal basis for doing so

Why we regularly share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our pupils with the Department for Education (DfE) either directly or via our local authority for the purpose of those data collections, under:

Examples for census:

- Section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Examples for Assessment and Reporting Arrangements:

- EYFSP - Section 40(2)(a) of the Childcare Act 2006 (Learning and Development Requirements) Order 2007 (S.I. 2007/1772)
- KS1 (including phonics) - section 87 of the Education Act 2002. Article 9 of The Education (National Curriculum) (Key Stage 1 Assessment Arrangements) (England) Order 20042
- KS2 - section 87 of the Education Act 2002. Article 11 of The Education (National Curriculum) (Key Stage 2 Assessment Arrangements) (England) Order 20032
- All data is transferred securely and held by DfE under a combination of software and hardware controls, which meet the current government security policy framework.
- For more information, please see 'How Government uses your data' section

Local Authorities

We may be required to share information about our pupils with the local authority to ensure that they can conduct their statutory duties under the Schools Admission Code, including conducting Fair Access Panels.

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact our DPL Judy Pope by email: office@stokenchurchprimary.bucks.sch.uk or telephone 01494 482112

Depending on the lawful basis above, you may also have the right to:

- Object to processing of personal data that is likely to cause, or is causing, damage or distress
- Prevent processing for the purpose of direct marketing
- Object to decisions being taken by automated means
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- A right to seek redress, either through the ICO, or through the courts

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

For further information on how to request access to personal information held centrally by DfE, please see the 'How Government uses your data' section of this notice.

Withdrawal of consent and the right to lodge a complaint
Where we are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting our DPL Judy Pope by email: office@stokenchurchprimary.bucks.sch.uk or telephone 01494 482112
If you would like to discuss anything in this privacy notice, please contact our DPO: Turn IT on by email: dpo@turniton.co.uk Telephone:01865 597620 option 3

How Government uses your data
The pupil data that we lawfully share with the DfE through data collections:

- Underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school
- Informs 'short term' education policy monitoring and school accountability and intervention (for example, Key Stage Assessments or Pupil Progress measures)
- Supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

Data collection requirements
To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools

The National Pupil Database (NPD)
Much of the data about pupils in England goes on to be held in the National Pupil Database (NPD).
The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department.

It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.
To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information

Sharing by the Department
The law allows the Department to share pupils' personal data with certain third parties, including:

- Schools
- Local authorities
- Researchers
- Organisations connected with promoting the education or wellbeing of children in England
- Other government departments and agencies
- Organisations fighting or identifying crime

For more information about the Department's NPD data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Organisations fighting or identifying crime may use their legal powers to contact DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, DfE typically supplies data on around 600 pupils per year to the Home Office and roughly 1 per year to the Police.

For information about which organisations the Department has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website: https://www.gov.uk/government/publications/dfe-external-data-shares

A11 – School Online Safety Policy: Electronic Devices - Searching Screening and Confiscation (updated with new DfE guidance – September 2022)

Introduction

The changing face of information technologies and ever-increasing Pupil 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 Pupils 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.

The Headteacher must publicise the school behaviour policy, in writing, to staff, parents/carers and Pupils at least once a year.

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.

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: Mr Stephen Sloan

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

Training/Awareness

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

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

Members of staff authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data/files from those devices should receive training that is specific and relevant to this role.
Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Policy Statements

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.

Pupils are allowed to bring mobile phones or other personal electronic devices to school and use them only within the rules laid down by the school.

If Pupils breach these rules:
The sanctions for breaking these rules can be found in the Electronic Devices 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 Pupil's consent for any item
- Searching without consent - Authorised staff may only search without the Pupil'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 Pupil is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for.
- The authorised member of staff should take reasonable steps to check the ownership of the mobile phone/personal electronic device before carrying out a search.
- The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the Pupil being searched.
- The authorised member of staff carrying out the search must be the same gender as the Pupil 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 Pupil being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a Pupil 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 Pupil 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 Pupil has or appears to have control – this includes desks, lockers and bags.

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

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

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

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

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

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

Care of Confiscated Devices

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

Audit/Monitoring/Reporting/Review

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

These records will be reviewed by the Safeguarding Governor termly.

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

A12 – Social Media Policy

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

Stokenchurch Primary School recognises the numerous benefits and opportunities which a social media presence offers. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the school, its staff, parents, carers and children.

Scope

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

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

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

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

Personal communications are those made via a 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.

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

Staff should refer to the school's AI Policy for guidance on using Artificial Intelligence in teaching and admin tasks, including how to manage data protection and ensure that pupils continue to produce their own original work.

Organisational control

Roles & Responsibilities

- SLT
  - Facilitating training and guidance on Social Media use.
  - Developing and implementing the Social Media policy
  - Taking a lead role in investigating any reported incidents.
  - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
  - Receive completed applications for Social Media accounts
  - Approve account creation

- Administrator/Moderator
  - Create the account following SLT approval
  - Store account details, including passwords securely
  - Be involved in monitoring and contributing to the account
  - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)

- Staff

- Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
- Attending appropriate training
- Regularly monitoring, updating and managing content he/she has posted via school accounts
- Adding an appropriate disclaimer to personal accounts when naming the school

Process for creating new accounts

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

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

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

Monitoring

School accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 48 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

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

Legal considerations

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

Handling abuse

- When acting on behalf of the school, respond to harmful and / or offensive comments swiftly and with sensitivity

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

Tone

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

- Engaging
- Conversational
- Informative
- Professional

Use of images

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

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

Personal use

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

- Pupils
    - Staff are not permitted to follow or engage with current or prior pupils of the school on any personal social media account unless the pupil is over 18
    - The school's education programme should enable the pupils to be safe and responsible users of social media
    - Pupils are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy

- Parents/Carers
    - If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use
    - The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website
    - Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures

Monitoring posts about the school

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

Appendix

Managing your personal use of Social Media:

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

Managing school social media accounts

The Do's

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

The Don'ts

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

A13 – Loaning School Equipment Policy

Statement of intent

Stokenchurch Primary School is dedicated to providing pupils with the best education possible. We understand the key role technology plays in maximising pupils' access to learning, as well as making lessons more exciting and engaging. We are committed to ensuring pupils have access to the necessary facilities to carry out their work, and believe it is important for pupils to be confident and competent users of equipment and the resources they access.

Staff, pupils and parents are expected to familiarise themselves with this policy and the school's Acceptable Use Agreement before loaning any school equipment. Copies of the agreement and this policy will be made available on request.

Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Data Protection Act 2018
- The UK General Data Protection Regulation
- DfE (2023) 'Keeping children safe in education 2023'
- DfE (2023) 'Meeting digital and technology standards in schools and colleges'

This policy operates in conjunction with the following school policies and documents:

- ICT Curriculum Policy
- Child Protection and Safeguarding Policy
- Online Safety Policy
- Data Protection Policy
- Debt Recovery Policy
- Technology Acceptable Use Agreements

Roles and responsibilities

Overall responsibility for oversight of the equipment and loaning process lies with the headteacher.
The headteacher will make decisions regarding:

- The allocation and provision of resources, taking into consideration recommendations from the designated equipment lead.
- How the equipment is utilised to benefit the aims and objectives of the school.

The Designated Equipment Lead (DEL/ IT Manager – Mrs Amy Whelan) is responsible for:

- Maintaining and running the equipment and the loans process.
- Resolving issues with equipment
- Carrying out checks on equipment before and after use
- Adjusting access rights and security privileges with the school's IT Manager
- Monitoring pupils' use of equipment with the IT Manager
- Reporting any signs of misuse and abuse of equipment to the headteacher
- Classifying and cataloguing resources, including undertaking a regular stock-take
- Storing of all equipment not out on loan safely
- Sending and drafting letters concerning overdue equipment to parents, teachers and senior management
- Sourcing, purchasing and cataloguing relevant equipment
- Demonstrating how to use equipment before use
- Liaising with ICT teachers to maximise pupils' use of the equipment
- Assisting the headteacher with their investigations if any equipment is lost or stolen
- Implementing this policy with the headteacher
- Implementing relevant parts of the school's ICT Curriculum Policy

The IT Manager is responsible for:

- Installing adequate malware protection on all loaned devices.
- Ensuring that the online protection offered on loaned devices, e.g. age-restricted content blockers, adheres to expectations outlined in the Online Safety Policy and Child Protection and Safeguarding Policy

The loaning procedure

Correspondence detailing the loans procedure and potential fines for late returns and damages will be sent to all parents.

Loans will be requested in writing, and pupils should give notice of at least five working days. Pupils must obtain their parents' signatures on their equipment request.

By loaning equipment, pupils and parents will agree to the terms of use as set out in this policy.
Once the request has been reviewed and accepted, pupils will be required to undergo training to use the equipment, including learning how to store and handle equipment, and how to undertake any maintenance, e.g. changing batteries – this training may be conducted virtually where necessary.

Only the pupil who has requested the equipment will be permitted to collect it. If the pupil is unable to collect the equipment from the school site, e.g. due to sickness, their parents should contact the school office to make alternative arrangements. If the equipment is no longer needed, pupils will notify the designated equipment lead/ IT Manager as early as possible to allow the equipment to be made available to someone else.

The maximum loan period is one week. Where a pupil requires loan of equipment for a longer period for learning purposes, e.g. where the pupil is learning remotely and must borrow a laptop to access the relevant materials, the headteacher and designated equipment lead will assess the pupil's situation and set an appropriate loan period which may be reviewed and extended where necessary.

Where a pupil is loaned electronic equipment for an extended period of time for remote learning purposes, their parents will be required to complete a Device Loan Agreement for Parents prior to the pupil taking the equipment off-site.

Pupils will require special consideration from the headteacher and designated equipment lead to loan equipment over weekends and school holidays. Overdue returns will incur a penalty fee of £10 per piece of equipment per day overdue – these costs will be outlined in the correspondence sent to parents.

When equipment is returned, the designated equipment lead will check all components and make sure it is in full working order. Pupils or their parents may request an extension to their existing loan period – this should be done in writing to the designated equipment lead. The headteacher and designated equipment lead will review any extension requests and extend the loan period by an appropriate number of days unless there is a reasonable justification not to do so, e.g. the equipment has been booked for loan to someone else. The headteacher and designated equipment lead are not required to extend the loan period by the length requested if this is not feasible; however, they will attempt to allow appropriate time for the requester to fulfil the tasks for which they require the loaned equipment.

Maintenance, service and storage

Servicing and storage of the equipment is the responsibility of the designated equipment lead, who will carry out visual checks before and after each use. Thorough checks of the equipment will be carried out termly. Checks for updates will be carried out on all laptops and tablets, including updates for malware protection and age-restriction settings. Regular stock-takes will be undertaken to ensure the whereabouts of each piece of equipment is known. All superficial damage will be noted in order to keep track of problems and to avoid wrongly charging someone for damage not caused by them.

Online safety

Online safety will be managed in line with the Child Protection and Safeguarding Policy and Online Safety Policy.
All loaned devices will be adequately equipped to keep pupils safe online, e.g. by having safe search filters in place, however it is a requirement that once the devices are connected to a home wi-fi network, the parent/carer is responsible for ensuring safe filters are on as this differs between home broadband providers. Pupils and their parents will not be permitted to remove any online safety features on the loaned device. The removal of these safety features will result in the termination of the loan, in line with the Acceptable Use Agreement. The IT Manager will ensure that the removal of online safety features on loaned devices is prohibited except by authorised users.

All users will be made aware that their activity on school devices will be monitored and subject to review to ensure appropriate use. If online safety concerns arise pupils will cease to use the loaned device and report it to the designated equipment lead as soon as possible. The designated equipment lead will report any online safety concerns relating to the use of loaned devices to the DSL. Concerns about the functionality of online safety features should be reported to the IT Manager and resolved as soon as possible. The device will not be returned to the pupil or made available for loan until the issue has been fully resolved and tested.

Routine checks to the school's filtering and monitoring systems will ensure that the system setup has not been changed or deactivated on any loaned devices. A log of all checks will be recorded. The school's filtering and monitoring provision for all devices will be reviewed at least annually to ensure it meets the needs of pupils and staff, reflects the school's use of technology and meets changing needs and potential risks.

Device security

All school devices will be protected with a correctly configured boundary, or software firewall. Firewall firmware will be kept up-to-date. Authentication will be required to access sensitive school or network data. Accounts will only be provided with the access required for the purposes for which the device is loaned.

Anti-malware software will be in place to protect all devices, and it will be kept up-to-date alongside associated files and databases. The IT Manager will ensure the school's anti-malware software:

- Is set up to scan files upon access, when downloaded, opened, or accessed from a network folder.
- Scans web pages as they are accessed.
- Prevents access to potentially malicious websites, unless risk-assessed, authorised and documented against a specific business requirement.

Staff and pupils will report any concerns about the security of the device, including possible cyber-attacks, to the IT Manager as soon as possible.

Lost, damaged and stolen goods

Pupils will be required to notify the designated equipment lead of any damage when returning the item – where the pupil is unable to do so, their parent/carer is responsible for notifying the designated equipment lead instead. Pupils will be held liable for any missing or damaged goods. Where the pupil's parent has signed the Acceptable Use Agreement on their child's behalf, the parent may also be liable for missing or damaged goods.
The designated equipment lead will test and carry out a visual check on all returned goods. If any damage is found, it will be assessed by the designated equipment lead. The following conditions will apply:

- If the damage is superficial, e.g. a scratch on the case or covering, there will be no charge.
- If the damage is more serious, the designated equipment lead will decide whether to incur a charge depending on the severity of the damage.

If the designated equipment lead and headteacher decide that the school requires a partial or full contribution towards repairs, a letter will be sent to the pupil's parents. The costs of the repairs will be reflective of the damage caused. Costs will be reviewed by the DEL and headteacher on a case-by-case basis. Fines for damage to equipment may be charged at a full replacement or repair cost.

In the event loan equipment is stolen, the pupil or their parent must immediately report the matter to the local police to obtain a crime reference number. The pupil or their parent should inform the DEL at the earliest opportunity, no later than the scheduled return date of the equipment, and give them the police crime reference number.

Pupils loaning equipment will be briefed on the security measures they must take.

Fines for late returns and damage

Fines for late returns will be incurred if any equipment is returned more than one day late. Payment plans may be put in place to aid the recovery of the debt – the implementation of a payment plan will be at the discretion of the headteacher.

In the event of late returns, the designated equipment lead will contact the pupil's parents to inform them that equipment has not been returned – during the phone call, the designated equipment lead will inform the parents that a fine has been administered for the late return.In the event of equipment being returned late, an invoice of the fine to be paid will be sent to the pupil's address. Fines will be charged at a rate of £10 per piece of equipment per day. Where an agreed payment plan is not in place and fines are not paid by the end of the Summer term, the debt will be passed on to an external debt collector.

Monitoring and review

This policy will be reviewed every two years by the headteacher and designated equipment lead. Any changes made to this policy will be communicated to all members of staff and parents. All members of staff directly involved in the use of the equipment will be required to familiarise themselves with this policy.

Legislation

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

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

A useful summary of relevant legislation can be found at: Report Harmful Content: Laws about harmful behaviours

Computer Misuse Act 1990

This Act makes it an offence to:

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

Data Protection Act 1998

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

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

The Data Protection Act 2018:

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

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

All data subjects have the right to:

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

Freedom of Information Act 2000

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

Communications Act 2003

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

Malicious Communications Act 1988

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

Regulation of Investigatory Powers Act 2000

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

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

Trade Marks Act 1994

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

Copyright, Designs and Patents Act 1988

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

Telecommunications Act 1984

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

Criminal Justice & Public Order Act 1994

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

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

Racial and Religious Hatred Act 2006

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

Protection from Harassment Act 1997

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

Protection of Children Act 1978

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

Sexual Offences Act 2003

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

Public Order Act 1986

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

Obscene Publications Act 1959 and 1964

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

Human Rights Act 1998

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

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

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

The Education and Inspections Act 2006

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

The Education and Inspections Act 2011

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

The Protection of Freedoms Act 2012

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

The School Information Regulations 2012

Requires schools to publish certain information on its website:
https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015

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

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence

in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

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
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_Advice_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/
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

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

A more comprehensive glossary can be found at the end of the UKCIS Education for a Connected World Framework.
This policy has been adapted with permission from the SWGfL Online Safety Policy Template.