Tatworth Primary School

ONLINE SAFETY POLICY

(This policy is included on our essential reading list)

This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).	
Responsibility for this online safety policy was delegated to the headteacher/SLT on 20 May 2021 who approved it:	October 2022
The implementation of this online safety policy will be monitored by the:	Online Safety Leader/Co-ordinator, teacher of ICT (Jonathan Goodman) who will report any issues immediately to SLT
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	October 2023
Should serious online safety incidents take place, the following external persons/agencies should be informed:	LA Safeguarding Officer, LADO, Police
The *governing body* will receive a report on the implementation of the Online Safety Policy generated by SLT (which will include anonymous details of online safety incidents) at regular intervals:	Once a year
Distribution	Website One-Drive
Source	SWGFL

2021	Introduced
2022	Revamp to SWGFL template rather than eLim

Contents

Scope of the Online Safety Policy

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

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

Tatworth Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Policy development, monitoring and review

This Online Safety Policy has been developed by

- Headteacher and senior leaders
- Online Safety Officer/Coordinator
- Online Security Director
- Administrative Staff
- IT Technician

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

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- *logs of reported incidents*
- *surveys/questionnaires of:*
    - *learners*
    - *parents and carers*
    - *staff.*

Policy and leadership

Responsibilities

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

Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to the Online Safety Lead.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff[2].
- The headteacher/senior leaders are responsible for ensuring that the Online Safety Lead, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The headteacher/senior leaders will receive regular monitoring reports from the Online Safety Lead.

Directors

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"

FPAR are responsible for reviewing the effectiveness of this policy e.g. by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges - questions from the Governing Body"

A member of the governing body will take on the role of Online Safety Governor to include:

- regular meetings with the Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- reporting to relevant Directors group/meeting
- membership of the school Online Safety Group
- occasional review of the filtering change control logs and the monitoring of filtering logs (where possible)

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

Online Safety Lead

The Online Safety Lead will:

- lead the Online Safety Group
- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL)
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated

Designated Safeguarding Lead (DSL)

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

> "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety). This should be explicit in the role holder's job description." … Training should provide designated safeguarding leads with a good understanding of their own role, … so they … are able to understand the unique risks associated with online safety and be confident that they have the

relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college."

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

- sharing of personal data [3]
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying.

The DSL will:

- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- have a leading role in establishing and reviewing the school online safety policies/documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- receive reports of online safety incidents[4] and create a log of incidents to inform future online safety developments
- provide (or identify sources of) training and advice for staff/Directors/parents/carers/learners
- liaise with (school/local authority/external provider) technical staff, pastoral staff and support staff (as relevant)
- meet regularly with the online safety director to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
- attend relevant meetings of Directors
- report regularly to senior leadership team.
- liaises with the relevant body.

Curriculum Leads

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

This will be provided through:

- Half-termly sessions during computer lessons that focus on internet safety.
- PHSE and SRE programmes
- A mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to the Headteacher, Senior Leaders or Online Safety Lead for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Safe Remote Learning Resource

- have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Network manager/technical staff

The network manager/technical staff (Soltech) 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 school 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 the Headteacher, Senior Leaders, or Online Safety Lead 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 A 'Technical Security Policy).
- monitoring software/systems are implemented and regularly updated as agreed in school policies

Learners

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

Parents and carers

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

The school will take every opportunity to help parents and carers understand these issues through:

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

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

- reinforcing the online safety messages provided to learners in school
- the use of their children's personal devices in the school (where this is allowed)
- digital and video images taken at school events
- access to parents' sections of the Learning Platform and on-line pupil records

Professional Standards

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

Policy

Online Safety Policy

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

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

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy

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

Acceptable use

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

Acceptable use agreements

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

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

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, 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 N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					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)					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways – further information here					
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 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	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

Consideration should be given for the following activities when undertaken for non-educational purposes:	Staff and Other Adults	Learners

	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awaren ess
Online gaming	X				x			
Online shopping/commerce				X	x			
File sharing		x			x			
Social media				x	x			
Messaging/chat				x	x			
Entertainment streaming e.g Netflix	X				X			
Use of video broadcasting e.g. Youtube			X		X			
Mobile phones may be brought into school		x			x			
Use of mobile phones for learning at school	X				X			
Use of mobile phones in social time		x			X			
Taking photos on mobile phones/cameras	x				x			
Use of other personal devices e.g tablets		x			x			
Use of personal e-mail in school or on school network/wifi			X		x			
Use of school e-mail for personal use	x				x			

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

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

Reporting and responding

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

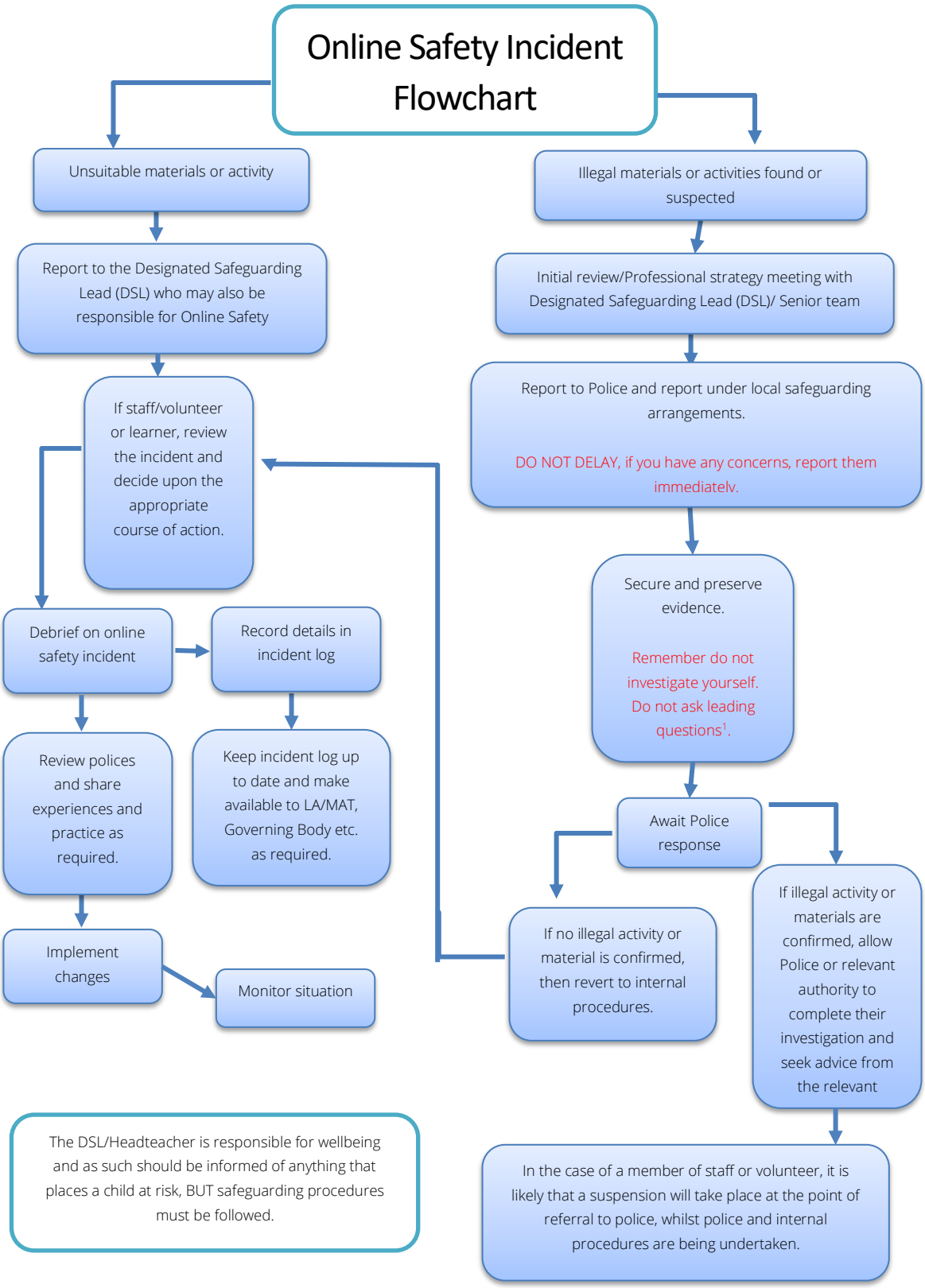
> *"School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. ..In order to do this, they should assume that sexual harassment and online sexual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

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

- there are clear reporting routes (via My Concern) which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart), the incident must be escalated through the agreed school safeguarding procedures.
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the LADO.
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
    - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
    - once this has been completed and fully investigated the appointed group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
        - internal response or discipline procedures
        - involvement by local authority
        - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively

- incidents should be logged on My Concern
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - staff, through regular briefings
    - learners, through assemblies/lessons
    - parents/carers, through newsletters, school social media, website
    - Directors, through regular safeguarding updates
    - local authority/external agencies, as relevant (The Ofsted Review into Sexual Abuse in Schools and Colleges suggested "working closely with Local Safeguarding Partnerships in the area where the school or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour"

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


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

School actions

It is more likely that 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 Learner Actions

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

Accidentally accessing offensive or pornographic material and failing to report the incident.		X			X			
Deliberately accessing or trying to access offensive or pornographic material.		X			X			
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.		X			X			
Unauthorised use of digital devices (including taking images)		X			X			
Unauthorised use of online services		X			X			
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		X			X			
Continued infringements of the above, following previous warnings or sanctions.		X			x			

Responding to Staff Actions

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

Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X		X				x
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers	X	x					
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail	x						
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	x						
Actions which could compromise the staff member's professional standing	X		x				
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X		x				
Failing to report incidents whether caused by deliberate or accidental actions	x						
Continued infringements of the above, following previous warnings or sanctions.	x				x		x

Online Safety Education Programme

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

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

> *"a carefully sequenced RSHE curriculum, based on the Department for Education's (DfE's) statutory guidance, that specifically includes sexual harassment and sexual*

violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of 'nudes'.."

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

- A planned online safety curriculum, including NSPCC material, is provided as part of Computing, PHSE, and other lessons and is regularly revisited
- Key online safety messages are reinforced as part of a planned programme of assemblies and pastoral activities
- Children are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information.
- Children are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Children are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school
- staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

- where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
- it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need

Contribution of Learners

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

- mechanisms to canvass learner feedback and opinion.
- appointment of digital leaders/school council
- learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns
- learners updating acceptable use agreements
- contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.

Staff/volunteers

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

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

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

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours
- the Online Safety Lead and Designated Safeguarding Lead 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/INSET days
- the Online Safety Lead will provide advice/guidance/training to individuals as required.

Directors

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

- attendance at training provided by the local authority or other relevant organisation (e.g., SWGfL)
- participation in school training / information sessions for staff or parents

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

Families

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

The school will seek to provide information and awareness to parents and carers through:

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

Technology

The school will ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection. A more detailed technical security policy template can be found in the Appendix A.

Soltech are contracted to support and maintain our IT. They are 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. They will also need to ensure that the relevant people named in the above sections are effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users are provided with a user name and password from County. The school administrator maintains a list of user names, but it is only the users who are aware of

their passwords. All 'users' are also included on County address book. Users are responsible for the security of their username and password.

- The "master/administrator" passwords for the school systems, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe)
- Soltech is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- We have a blanket restrictive policy that may be bypassed by staff (via a user name and password). The school's filtering administrator has the ability to add exceptions to the filtering list which would then apply to both children and staff.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has differentiated user-level between staff and the children.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person..
- Appropriate security measures are in place, for example **usernames / passwords etc., up-to-date software, regular patches applied, network access permissions,** to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. 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 devices are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Filtering

- the school filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
- the school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre Appropriate filtering.

If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

Monitoring

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

> "It is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place …governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the … risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. "

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

- The school monitors all network use across all its devices and services.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. There is a staff lead responsible for managing the monitoring strategy and processes.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

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

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- *pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.*

- *where possible, school technical staff regularly monitor and record the activity of users on the school technical systems*
- *use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)*

Technical Security

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

- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually.
- all users (adults and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password
- the master account passwords for the school systems are kept in a secure place, e.g. school safe.
- passwords should be long.
- records of learner usernames and passwords for learners in Key Stage 1 or younger can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.
- password requirements for learners at Key Stage 2 and above should increase as learners progress through school
- Soltech is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.

- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint (anti-virus) software.
- an agreed policy is in place for the provision of temporary access of 'guests', (e.g., trainee teachers, supply teachers, visitors) onto the school systems
- an agreed policy is in place regarding the extent of personal use that users (staff / learners / community users) and their family members are allowed on school devices that may be used out of school
- an agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices
- an agreed policy is in place regarding the use of removable media (e.g., memory sticks/CDs/DVDs) by users on school devices.
- systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured.

Mobile technologies

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

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

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

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

The school allows:

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

Social media

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

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

All schools and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online,

discriminate on the grounds of sex, race, or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

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

School staff should ensure that:

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

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

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

Personal use

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

- personal communications which do not refer to or impact upon the school are outside the scope of this policy
- where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- the school permits reasonable and appropriate access to personal social media sites during school hours

Monitoring of public social media

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

Digital and video images

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

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm (select/delete as appropriate):

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies. Guidance can be found on the SWGfL Safer Remote Learning web pages and in the DfE Safeguarding and remote education
- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes

- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that learners are appropriately dressed
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media.
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- images will be securely stored in line with the school retention policy
- learners' work can only be published with the permission of the learner and parents/carers.

Online Publishing

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

- Public-facing website
- Social media
- Online newsletters

The school website is hosted by Polkadot Education. The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal

information – ensuring that there is least risk to members of the school community, through such publications.

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

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

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

Data Protection

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

The school:

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

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

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

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

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any school personal data to personal devices.
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

Appendix

The appendices are as follows:

A Technical Security Policy
B Parent/Carer AUP, inc Pupils
C Younger Pupils AUP
D Staff and Volunteer AUP
E Electronic Devices – Searching Screening and Confiscation (new DfE guidance from September 2022)

Appendix A

Technical Security Policy

(including filtering and passwords)

Ratified by:	SLT
Date:	17 May 2022
Next Review:	Spring 2023

Distribution:	OneDrive
Source:	eLim Consultation with DPO and Soltech
Related Documents	Online Safety Policy Data Protection Policy Acceptable Use Agreements Child Protection (Safeguarding) Policy Privacy Notices

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the *school infrastructure/network* is as safe and secure as is reasonably possible and that:

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

We engage the services of Soltech who carry out all of the online safety measures under the instructions of the school. It is the responsibility of the school to ensure that Soltech is fully aware of the school's online safety policy/data protection/acceptable use agreements and follows the school's instructions at all times.

Scope of the policy

This policy should be read alongside the following Tatworth School documents:

- Data Protection Policy
- Online Safety Policy
- Safeguarding Policy
- Privacy notices for pupils/parents

This policy reflects the requirements of Tatworth School to comply with the following legislation

- The UK General Data Protection Regulation
- The Data Protection Act 2018
- The Computer Misuse Act 1990
- Keeping Children Safe in Education 2021

This policy applies to all staff including school, agency staff, contractors, work experience students and volunteers.

Responsibilities

The school has a contract with Soltech to provide support for technical security.

Technical Security

Responsibilities of the School

The school will:

- be responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.
- ensure that the relevant people receive guidance and training and are effective in carrying out their responsibilities
- ensure that technical systems are managed in ways which meet recommended technical requirements of Somerset Local Authority as stated by the SCCICT Team https://www.sccict.co.uk/
- ensure that there are regular reviews and audits of the safety and security of school technical systems
- ensure that servers, wireless systems and cabling are securely located and physical access restricted
- ensure that appropriate security measures 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's systems and data
- ensure that responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff
- by liaison with the network manager/technical support provider, ensure that all users have clearly defined access rights to school/academy technical systems
- by liaison with the network manager/technical support provider, ensure that details of the access rights available to groups of users are recorded by the IT technician and are reviewed, at least annually, by the senior leadership team
- by liaison with the IT technician, ensure that an appropriate system is in place for users to report any actual/potential technical incident to the nominated in-school lead
- by liaison with the IT technician, ensure that an agreed policy is in place and implemented regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on school/academy devices that may be used out of school/academy
- by liaison with the IT technician, ensure that an agreed policy is in place and implemented regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school/academy devices
- by liaison with the IT technician, ensure that the school infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc.

Responsibilities of network manager/technical support provider

- The responsibilities of the IT technician are primarily listed in the contract with the provider.
- In addition to the other requirements of this policy, the IT technician will:
    - Read, sign, and follow the school acceptable user agreement for technicians
    - regularly monitor and record the activity of users on the school's technical systems (add details of the monitoring programs that are used)
    - ensure 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)
    - ensure that remote management tools are used by staff to control workstations and view users' activity
    - ensure that mobile device security and management procedures are in place (where mobile devices are allowed access to school systems).
    - ensure provision for temporary access of "guests", (e.g., trainee teachers, supply teachers, visitors) onto the school/academy system
    - enforce the school agreed policy regarding the downloading of executable files and the installation of programs on school devices by users

Responsibilities of staff

This policy applies to all staff including school, agency staff, contractors, work experience students and volunteers.

School staff will:

- read, sign, and follow the school's acceptable user agreement
- read and follow the school's Data Protection policy
- complete the National Cyber Security Centre's online staff training
- ensure that school devices are locked when the staff member is out of the room;
- ensure that passwords for school systems are not shared with other staff members or pupils
- if using removable storage (laptop, tablet, USB memory stick) ensure that this is approved by the school, and is password protected and encrypted.
- when working from home, ensure appropriate security is in place to protect equipment or information not be used by non-school staff. This will include ensuring equipment and information is kept out of sight.
- ensure that any machine not routinely connected to the school network, is brought in regularly to receive updates by the IT team.
- ensure that all school data is stored on the school network or portal, not kept solely on the laptop

- ensure that all locally stored data is synchronised with the school network server on a frequent basis

- ensure that school-issued laptops are available for inspection by school-authorised personnel (e.g. the office administrator) at any time

- not attempt to access any network drives or areas to which they do not have authorised permission from the school

- use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, or Trojan horse code

- **in the event of a suspected cyberattack.** turn off device and inform the school office and do not connect device to the school network until it has been checked by the It technician

Password Security

Policy Statements:

Staff passwords

- All school networks and systems are protected by secure passwords.
- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available will be reviewed, at least annually, by the senior leadership team as detailed above.
- All users (adults and learners) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- Passwords must not be shared with anyone
- Passwords should be long. Good practice highlights that passwords over 12 characters in length are more difficult to compromise than shorter passwords. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school/academy
- Passwords must not include names or any other personal information about the user that might be known by others
- Passwords must be changed on first login to the system
- Passwords should not be set to expire as long as they comply with the above but should be unique to each service the user logs into.

Learner passwords

- Foundation Stage and KS1 learners will have simple passwords with a six-character maximum, without special characters

- Records of learner usernames and passwords for Foundation Stage/KS1 pupils can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.
- Password requirements for learners at Key Stage 2 and above will increase as pupils progress through the school.
- All learners will be required to change their password if it is compromised. Passwords will not be regularly changed but should be secure and unique to each account.
- Learners will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

Administrator passwords

- Each administrator will have an individual administrator account, as well as their own user account with access levels set at an appropriate level. These accounts will have two-factor authentication in place
- Administrator passwords for school systems should also be kept in a secure place e.g., school/academy safe. This account and password should only be used to recover or revoke access. Other administrator accounts should not have the ability to delete this account. (A school/academy should never allow one user to have sole administrator access)
- Any digitally stored administrator passwords should be hashed using a suitable algorithm for storing passwords (e.g. Bcrypt or Scrypt).

Setting and resetting passwords

- It is good practice that where passwords are used there is a user-controlled password reset process to enable independent, but secure re-entry to the system. This ensures that only the owner has knowledge of the password.
- Where user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users will be allocated by IT technician. The password generated by this change process should be system generated and only known to the user. This password should be temporary, and the user should be forced to change their password on first login. The generated passwords should also be long and random.
- Where automatically generated passwords are not possible, then an age-appropriate password generator e.g. www.dinopass.com or https://passwordsgenerator.net should be used to provide the user with their initial password. There should be a process for the secure transmission of this password to limit knowledge to the password creator and the user. The password should be temporary and the user should be forced to change their password on the first login
- Requests for password changes should be authenticated by the office manager to ensure that the new password can only be passed to the genuine user
- Arrangements are in place to provide visitors with appropriate access to systems which expires after use. (For example, providing a pre-created user/password combinations that can be allocated to visitors, recorded in a log, and deleted from the system after use.)
- In good practice, the account is “locked out” following six successive incorrect log-on attempts.
- Passwords shall not be displayed on screen and shall be securely hashed when stored (use of one-way encryption).

Training/Awareness:

- It is essential that users are aware of the need to keep the school’s systems safe from harm

- This will be done at an age-appropriate level e.g., for young learners, staff will talk about the importance of keeping your password safe (see the Online Safety policy for further details).
- It will also be done through staff modelling appropriate use e.g., not leaving devices logged on, and not sharing passwords with classroom assistants
- Members of staff will be made aware of this policy:
    - at induction
    - through the online safety policy and password security policy
    - through the acceptable use agreement
- Learners will be made aware of this policy:
    - in lessons (e.g. online safety lessons)
    - through the acceptable use agreement
- Staff will be expected to complete the National Cyber Security Centre's online training as listed above, and will receive annual refresher training in data protection

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

- The school has overall responsibility to ensure that the filtering systems is robust and complies with the requirements of Keeping Children Safe in Education 2021. Soltech will manage the system on a day-to-day basis, as instructed by the Headteacher or Deputy Headteacher, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.
- To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:
    - **be logged in change control logs**
    - **be reported to a second responsible person**:
    - *be reported to the DSL regularly in the form of an audit of the change control logs*
- All users have a responsibility to report immediately to the DSL any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.
- Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Policy Statements

- Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.
- *The school maintains and supports the managed filtering service provided by the Internet Service Provider*
- *The school has provided enhanced/differentiated user-level filtering through the use of RM filtering programme. (allowing different filtering levels for different groups of users – staff/children)*
- *In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher or DSL*
- *Mobile devices that access the school/academy internet connection (whether school/academy or personal devices) will be subject to the same filtering standards as other devices on the school systems*
- *Any filtering issues should be reported immediately to the filtering provider.*
- *Requests from staff for sites to be removed from the filtered list will be considered by the technical staff* (James Willis, IT Technician) and Headteacher*. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.*

Education/Training/Awareness

- Pupils will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.
- Staff users will be made aware of the filtering systems through:
    - the acceptable use agreement
    - induction training
    - staff meetings, briefings, Inset.
- Parents will be informed of the school's filtering policy through the acceptable use agreement and through online safety awareness sessions/newsletter etc.

Changes to the Filtering System

- Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the DSL who will decide whether to make school level changes (as above).

Monitoring of the filtering system

- No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school

equipment as indicated in the school online safety policy and the acceptable use agreement.

Audit/Reporting

- Logs of filtering change controls and of filtering incidents will be made available to:
    - Soltech; DSL or Deputy DSL
    - Online Safety Governor
    - External Filtering provider/Local Authority/Police on request

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

Reporting policy incidents

Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data should raise the matter with the Headteacher or Chair of Governors.

Monitoring and evaluation of this policy

This policy will be monitored and reviewed in line with the school's policy review procedure.

The school will monitor the implementation of the policy through:

- annual data protection walks around the school site to ensure that the school's requirements are followed by staff
- annual back-up and restore check of data
- regular spot checks of school systems and devices
- checks against national cyber security auditing systems e.g. the DfE Cyber Secure tool

APPENDIX B

TATWORTH PRIMARY SCHOOL
Parent/Carer
Acceptable Use of Technology Policy

(January 2022)

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

This acceptable use policy is intended to ensure:

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

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

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

Permission Form

Parent/Carers Name: .....

Student(s)/Pupil(s) Name: .....

As the parent/carer of the above children, I give permission for my son/daughter to have access to the internet and to ICT systems at school.

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

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

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

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

Please note that the school office staff will have access to this form and the information that you have shared therein. A hard copy of the form will be held in your child's file until they leave the school. At this point their personal files will be shredded, unless there is legitimate reason not to do so.

Signed: .....

Date: .....

Pupil Acceptable Use Agreement

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

TATWORTH PRIMARY SCHOOL
Pupils'
Acceptable Use of Technology Policy

(January 2022)

Technology is a great tool to support learning, find information and to communicate and share with others.

The school encourages its appropriate, effective and safe use. All users of technology in the school must agree to certain rules and will only use the equipment and software as instructed.

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I will follow the agreed rules when using technology including the internet. And know that if I break the rules I might not be allowed to use a computer/tablet
- I understand that the school will monitor my use of computers and other technology.
- I understand that the school may investigate incidents that cause upset or harm taking place outside school.
- I recognise if I misuse technology, it has an effect on others and consequences for me.
- I will report any suspected misuse or problems to a trusted adult in the school.
- I will think about the ways I use technology so that it will not affect my physical or mental health.

Online bullying

- I understand that the school will not accept bullying in any form.
- I will be careful to check that anything I write or say in documents, messages or online is not offensive or could cause hurt or embarrassment.
- I understand that I should report any incidents of bullying.

Signed (child): .....

Use of internet

I will not try to access sites that are blocked or that are unsuitable for use in school.
I will carefully check information I use for my learning.
I will report any worrying or damaging materials I come across.

Personal mobile devices

I will only use personal mobile devices when I have permission from by my teachers.

Name _____

Signed _____

Class _____ Date _____

APPENDIX C

TATWORTH PRIMARY SCHOOL
Younger Pupils'
Acceptable Use of Technology Policy

(November 2021)

Technology is a great tool to support learning, find information and to communicate and share with others.

The school encourages its appropriate, effective and safe use. All users of technology in the school must agree to certain rules and will only use the equipment and software as instructed.

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I will follow the agreed rules when using technology including the internet. And know that if I break the rules I might not be allowed to use a computer/tablet
- I understand that the school will monitor my use of computers and other technology.
- I understand that the school may investigate incidents that cause upset or harm taking place outside school.
- I recognise if I misuse technology, it has an effect on others and consequences for me.
- I will report any suspected misuse or problems to a trusted adult in the school.
- I will think about the ways I use technology so that it will not affect my physical or mental health.

Online bullying

- I understand that the school will not accept bullying in any form.
- I will be careful to check that anything I write or say in documents, messages or online is not offensive or could cause hurt or embarrassment.

- I understand that I should report any incidents of bullying.

Signed (child): .....

Use of internet

I will not try to access sites that are blocked or that are unsuitable for use in school.
I will carefully check information I use for my learning.
I will report any worrying or damaging materials I come across.

Personal mobile devices

I will only use personal mobile devices when I have permission from by my teachers.

Name _____

Signed _____

Class _____ Date _____

APPENDIX D

TATWORTH PRIMARY SCHOOL

Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

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

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school/academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for *children* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the *school* will monitor my use of the school digital technology and communications systems.

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

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies
- I will only communicate with children and parents/carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the *school*:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school/academy policies.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school/academy policies.
- I will not disable or cause any damage to school/academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/Academy/LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school/academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

- I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school/academy
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include: a warning, a suspension, referral to Governors/directors and/or the Local Authority and in the event of illegal activities the involvement of the police.

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

Staff/Volunteer Name: .....

Signed: .....

Date: .....

Appendix

Electronic Devices - Searching Screening and Confiscation

(updated with new DfE guidance – September 2022)

Introduction

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

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

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

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

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

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

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

Our behaviour policy is posted onto our school website. Copies may also be requested from the school office.

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 Headteacher will need to authorise those staff who are allowed to carry out searches.

This policy has been written by and will be reviewed by: SLT

The Headteacher has authorised the SLT to carry out searches for and of electronic devices and the deletion of data/files on those devices.

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

Training/Awareness

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

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

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

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

Policy Statements

Search:

This policy refers only to the searching for and of electronic devices and the deletion of data/files on those devices.

Learners are only allowed to bring mobile phones or other personal electronic devices to school in exceptional circumstances. They may not use them during the school day and must leave them in the school office.

If learners breach these roles:

The sanctions for breaking these rules can be found in the Online Security Policy.

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

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

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

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

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

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

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

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

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

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

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

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

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

Electronic devices

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

- Electronic devices, including mobile phones, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, indecent images of children, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour.
- As with all prohibited items, staff should first consider the appropriate safeguarding response if they find images, data or files on an electronic device that they reasonably suspect are likely to put a person at risk
- Staff may examine any data or files on an electronic device they have confiscated as a result of a search .if there is good reason to do so (defined earlier in the guidance as)
    - poses a risk to staff or pupils;
    - is prohibited, or identified in the school rules for which a search can be made or
    - is evidence in relation to an offence.
- If the member of staff conducting the search suspects they may find an indecent image of a child (sometimes known as nude or semi-nude images), the member of staff should never intentionally view the image, and must never copy, print, share, store or

save such images. When an incident might involve an indecent image of a child and/or video, the member of staff should confiscate the device, avoid looking at the device and refer the incident to the designated safeguarding lead (or deputy) as the most appropriate person to advise on the school's response. Handling such reports or concerns can be especially complicated and schools should follow the principles as set out in Keeping children safe in education. The UK Council for Internet Safety also provides the following guidance to support school staff and designated safeguarding leads: Sharing nudes and semi-nudes: advice for education settings working with children and young people.

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

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

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

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

Further guidance on reporting the incident to the police and the preservation of evidence can be found in the SWGfL flow chart in the main School Policy document. Local authorities/local safeguarding partnerships may also have further guidance, specific to their area.

A record should be kept of the reasons for the deletion of data/files.

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 Headteacher will ensure that full records are kept of incidents involving the searching for and of electronic devices and the deletion of data/files

These records will be reviewed by the Online Safety Director at regular intervals.

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