

# **St Neot Community Primary School**

## **Online Safety Policy**

This policy applies to all members of the school community (including staff, children, volunteers, parents and carers, visitors) 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.

Version: [3}

Date created: [March 2023}

Next review date: [March 2024]

## Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of St Neot Community Primary School and Nursery to safeguard members of our school community online in accordance with statutory guidance and best practice.

This Online Safety Policy applies to all members of the school community (including staff, children, volunteers, parents and carers, visitors) 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.

St Neot Community Primary School and Nursery 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 and approved by the online safety committee made up of:

- Head teacher
- ICT/Online Safety Co-ordinator
- Governors
- School Secretary
- Online Safety Governor
- School Council

## Schedule for development, monitoring and review

This Online Safety Policy was approved by the school governing body on:	14 <sup>th</sup> March 2023
The implementation of this Online Safety Policy will be monitored by:	The Online Safety Governor
Monitoring will take place at regular intervals:	Termly by ICT/Online Safety Co-ordinator
The governing body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Termly by ICT/Online Safety Co-ordinator
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:	Annually – March 2024
Should serious online safety incidents take place, the following external persons/agencies should be informed:	Chair of Governors, LA Safeguarding Officer, Police as appropriate

## Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- logs of reported incidents
- monitoring logs of internet activity (including sites visited)

## Policy and leadership

### Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these

become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

## Head teacher and senior leaders

- The head teacher 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 ICT/Online Safety Lead.
- The head teacher/online safety governor should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The head teacher/online safety governor are responsible for ensuring that ICT/Online Safety Lead, school secretary, school council, 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 head teacher/online safety governor 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 head teacher/online safety governor will receive regular monitoring reports from the ICT/ Online Safety Lead.

## Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy

This review will be carried out by the Governors receiving regular information about online safety incidents and the monitoring reports. A member of the Governing board has taken on the role of Online Safety Governor to include:

- regular meetings with the ICT/Online Safety co-ordinator
- 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)

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

## ICT/Online Safety Co-ordinator

The ICT/Online Safety co-ordinator will:

- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL)
- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- 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 and create a log of incidents to inform future online safety developments
- provide training and advice for staff/governors
- meet regularly with the online safety governor/head teacher/DSL to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
- report regularly to head teacher

## Designated Safeguarding Lead (DSL)

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

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

## 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 policy (AUP)

- they immediately report any suspected misuse or problem to Online Safety Co-ordinator for investigation/action, in line with the school safeguarding procedures
- all digital communications with children 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 children 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 and implement current policies regarding these devices
- in lessons where internet use is pre-planned children 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
- have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc

## Children

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

## Parents and carers

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

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the children's 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
- 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 children in school

## Online Safety Group

The Online Safety Group has the following members:

- ICT/Online Safety Co-ordinator
- Designated Safeguarding Lead
- Governors
- Online safety governor
- School Council
- Children
- Parents/carers

Members of the Online Safety Group will assist the Online Safety Co-ordinator with:

- the production/review/monitoring of the school Online Safety Policy/documents
- reviewing network/filtering/monitoring/incident logs, where possible
- encouraging the contribution of children to staff awareness, emerging trends and the school online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.

## 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 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 children in the digital world
- describes how the school will help prepare children to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels
- is published on the school website.

## Acceptable use

### Acceptable use agreements

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

- staff induction and handbook
- posters/notices around where technology is used
- communication with parents/carers
- 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:	<b>Any illegal activity for example:</b> <ul style="list-style-type: none"> <li>• Child sexual abuse imagery</li> <li>• Child sexual abuse/exploitation/grooming</li> <li>• Terrorism</li> <li>• Encouraging or assisting suicide</li> <li>• Offences relating to sexual images i.e., revenge and extreme pornography</li> <li>• Incitement to and threats of violence</li> <li>• Hate crime</li> <li>• Public order offences - harassment and stalking</li> <li>• Drug-related offences</li> <li>• Weapons / firearms offences</li> <li>• Fraud and financial crime including money laundering</li> </ul>					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	<ul style="list-style-type: none"> <li>• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised)</li> <li>• Gaining unauthorised access to school networks, data and files, through the use of computers/devices</li> <li>• Creating or propagating computer viruses or other harmful files</li> <li>• Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)</li> <li>• Disable/Impair/Disrupt network functionality through the use of computers/devices</li> <li>• Using penetration testing equipment (without relevant permission)</li> </ul>					X
Users shall not undertake activities that are not illegal but are	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUPs)				X	

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
classed as unacceptable in school policies:	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				Children			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Online gaming	X				X			
Online shopping/commerce			X		X			
File sharing			X		X			
Social media			X		X			
Messaging/chat			X		X			

Use of video broadcasting, e.g. YouTube			X		X			
Mobile phones may be brought to school		X						X
Use of mobile phones for learning at school	X				X			
Use of mobile phones in social time at school			X		X			
Taking photos on mobile phones/cameras				X	X			
Use of other personal devices, e.g. tablets, gaming devices	X				X			

Use of personal e-mail in school, or on school network/wi-fi			X		X			
Use of school e-mail for personal e-mails	X				X			

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

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school
- any digital communication between staff and children 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 children.

## Reporting and responding

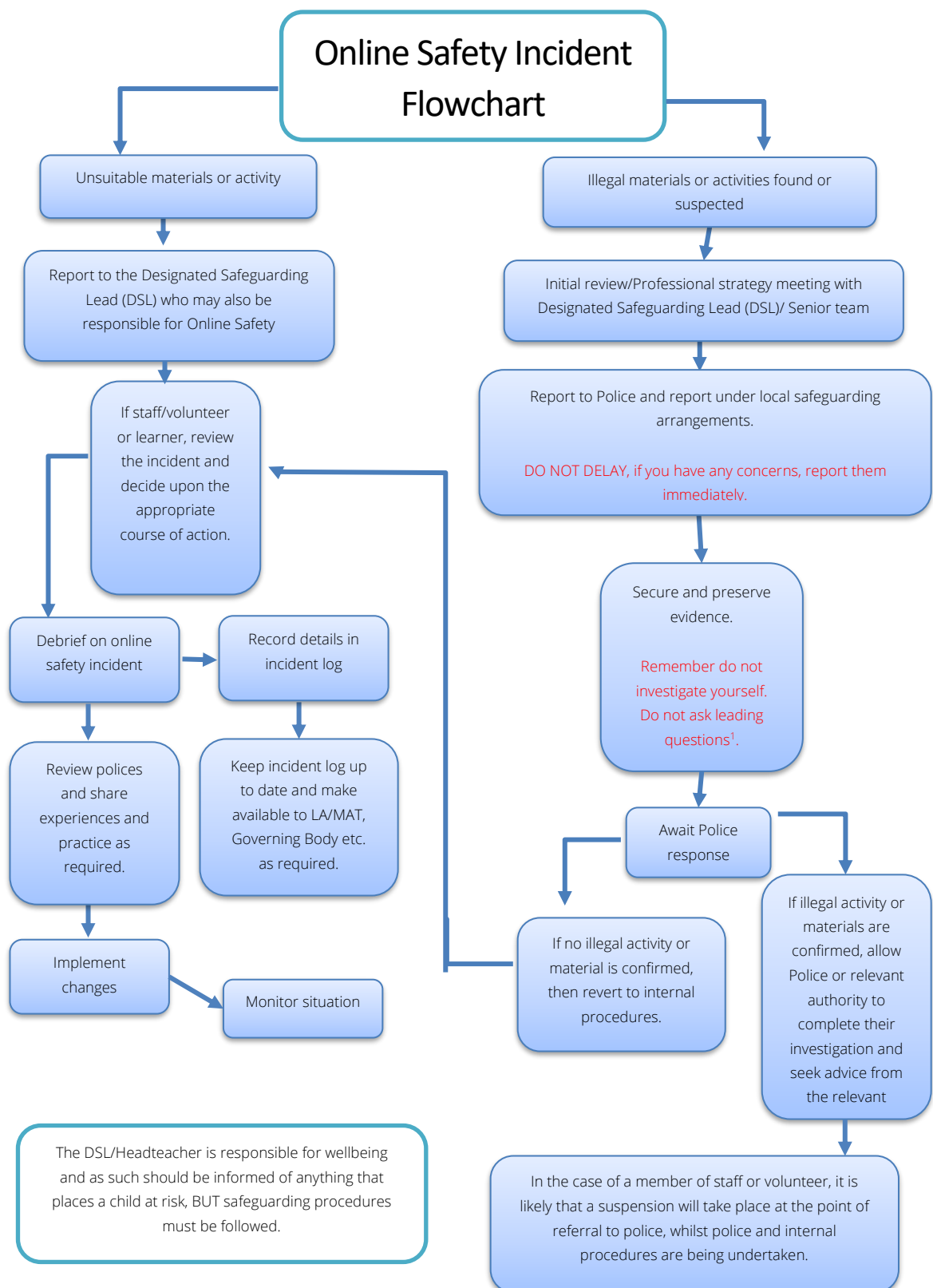
The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.

- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, 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, the incident must be escalated through the agreed school safeguarding procedures.
- any concern about staff misuse will be reported to the Head teacher, unless the concern involves the Head teacher, in which case the complaint is referred to the Chair of Governors.
- 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 children and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
  - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
  - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
  - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - internal response or discipline procedures
    - involvement by local authority
    - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police;

- 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 to:
  - the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
  - staff, through regular briefings
  - children, through assemblies/lessons
  - parents/carers, through newsletters, website
  - governors, through regular safeguarding updates
  - local authority/external agencies, as relevant

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





## School actions

It is more likely that 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	Refer to Head teacher	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/carers	Remove device/network/internet access rights	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X	X					
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords	X						X	
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			X		X	X
Unauthorised downloading or uploading of files or use of file sharing.	X	X					X	

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

## Responding to Staff Actions

<b>Incidents</b>	Refer to local authority	Refer to Police	Refer to I T/Online Safety Co-ordinator	Issue a warning	Suspension
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)</b>	<b>X</b>	<b>X</b>	<b>X</b>		
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	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	

Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.			X	X	X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature				X	X
Using personal e-mail/social networking/messaging to carry out digital communications with children and parents/carers				X	
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail				X	X
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner				X	
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

# Online Safety Education Programme

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

- A planned online safety curriculum for all year groups matched against a nationally agreed framework
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to children at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- children 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 children 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 children are allowed to freely search the internet, staff should be vigilant in supervising the children 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 Children

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

- mechanisms to canvass learner feedback and opinion.
- appointment of digital leaders/anti-bullying ambassadors/peer mentors
- the Online Safety Group has learner representation
- children designing/updating acceptable use agreements

## Staff/volunteers

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

- all new staff will 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 Co-ordinator and Designated Safeguarding Lead will receive regular updates through attendance at external training events, and by reviewing guidance documents released by relevant organisations
- this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- the Online Safety Co-ordinator will provide advice/guidance/training to individuals as required.

## Governors

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

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

## Families

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 parent consultation
- the children – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by children leading sessions at parent/carer consultation
- letters, newsletters, website, learning platform,
- high profile events / campaigns e.g. Safer Internet Day

## Technology

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

## Filtering

- the school filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
- the school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre
- access to online content and services is managed for all users
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content
- there is a clear process in place to deal with requests for filtering changes
- the school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/children, etc.)

- filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.
- where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

## Monitoring

The 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 and will be reviewed, at least annually, by ICT/Online Safety Co-Ordinator.
- all users (adults and children) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by ICT/Online Safety Co-ordinator who will keep an up-to-date record of users and their usernames
- passwords should be long
- records of learner usernames and passwords for children in Key Stage 1 or younger can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. Password complexity for younger children may be reduced (for example 6 character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged
- password requirements for children at Key Stage 2 and above should increase as children progress through school
- ICT/Online Safety Co-ordinator is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates
- 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,) onto the school systems
- an agreed policy is in place regarding the extent of personal use that users (staff / children) 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
- systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured.

## Mobile technologies

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

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

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

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

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

The school acceptable use agreements for staff, children, volunteers, 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	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No	Yes	Yes
Full network access	Yes	Yes	Yes			
Internet only						
No network access						

School owned/provided devices:

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

## Personal devices

- which users are allowed to use personal mobile devices in school (staff/children/visitors)
- restrictions on where, when and how they may be used in school
- if used in support of learning, how staff will plan their lessons around the potential variety of device models and different operating systems
- storage
- whether staff will be allowed to use personal devices for school business
- levels of access to networks/internet (e.g., access, or not, to internet/guest wi-fi/network)
- network/broadband capacity
- technical support (this may be a clear statement that no technical support is available)
- filtering of the internet connection to these devices and monitoring the access
- management of software licences for personally owned devices.
- data protection
- taking/storage/use of images
- liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility)
- identification/labelling of personal devices
- how visitors will be informed about school requirements
- how education about the safe and responsible use of mobile devices is included in the school online safety education programmes
- how misuse will be dealt with

## Social media

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

School staff should ensure that:

- no reference should be made in social media to children, 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

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

- the school may use live-streaming or video services in line with national and local safeguarding guidance / policies.

- when using digital images, staff will inform and educate children about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those children whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other children 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 children are appropriately dressed
- children must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include children will be selected carefully and will comply with Online Safety Policy
- children's 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 children are taken for use in school or published on the school website/social media. Permission is not required for images taken solely for internal purposes
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- images will be securely stored in line with the school retention policy

## Online Publishing

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

- Public-facing website
- Online newsletters

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

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

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

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

## 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. The school may also wish to appoint a Data Manager and Systems Controllers to support the DPO
- 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, 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
- 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 GDPR breaches to ICT/Online Safety Co-ordinator within 72 hours
- has a Freedom of Information Policy which sets out how it will deal with FOI requests

**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
- will not transfer any school personal data to personal devices. Procedures should be in place to enable staff to work from home (i.e. VPN access to the school network, or a work laptop provided).
- use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

**Outcomes**

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

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school’s online safety awareness raising
- online safety policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate

Every effort has been made to ensure that the information included in this document is accurate.