Online Safety

A.Woolf@skeltonprimaryschool.co.uk

Autumn 2023

The difference between try and triumph is UMPPHHH!

Original date approved	Autumn 2023
Current date approved	Click or tap to enter a date.
Date of next review	Autumn 2024
Policy owner	A.Woolf@skeltonprimaryschool.co.uk
Policy type	Non statutory

Document History:			
Version	**Date of review**	**Author**	**Note of revisions**

Online Safety

Contents

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Skelton 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).

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

Policy development, monitoring and review

This Online Safety Policy has been developed by the:

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

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

Schedule for development, monitoring and review

This Online Safety Policy was approved by the *school governing body on:*	*2023*
The implementation of this Online Safety Policy will be monitored by:	*A.Woolf*
Monitoring will take place at regular intervals:	*Annually*
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:	*Annually*
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:	*Jan 24*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*LA safeguarding officer,* *police*

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- *logs of reported incidents on Cpoms*
- *monitoring logs of internet activity (including sites visited)*
- *internal monitoring data for network activity*
- *surveys/questionnaires of:*
    - *learners*
    - *parents and carers*
    - *staff.*

Policy and leadership

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

Acceptable use

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

Acceptable use agreements

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:	**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					x

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	• 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					
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) 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***					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

Consideration should be given for the following activities when undertaken for **non-educational purposes:**	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Online gaming	X				X			
Online shopping/commerce			X		X			
File sharing	X				X			
Social media	X				X			
Messaging/chat		X			X			
Entertainment streaming e.g. Netflix, Disney+	X				X			

Use of video broadcasting, e.g. YouTube, Twitch, TikTok	X				X			
Mobile phones may be brought to school		X				X Left in office		
Use of mobile phones for learning at school	X				X			
Use of mobile phones in social time at school		X in selected areas			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 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.

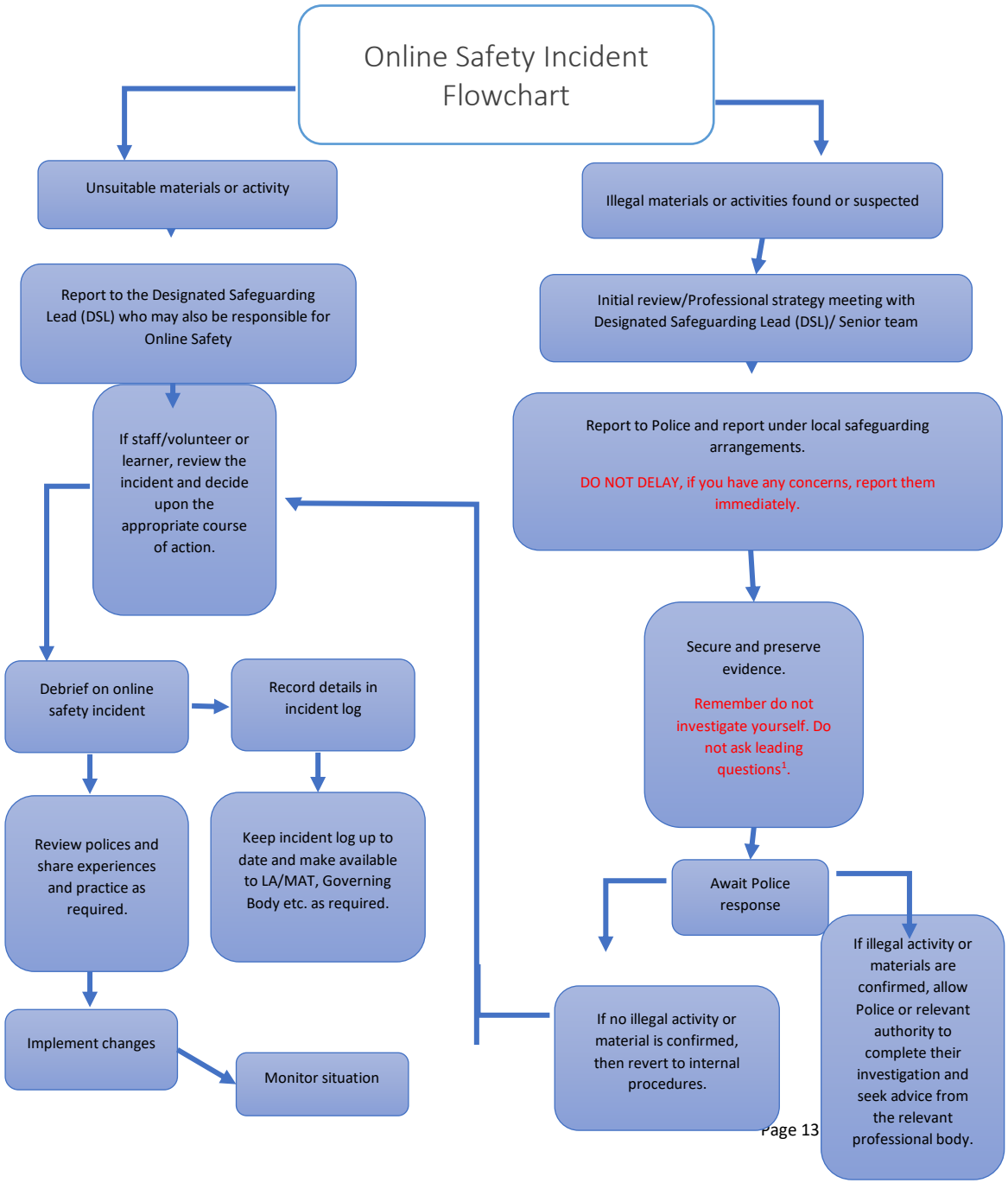
Reporting and responding

The 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/ whistleblowing procedures.**
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority.
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
    - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form

- once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - internal response or discipline procedures
    - involvement by local authority / MAT (as relevant)
    - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged on cpoms.
- 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:
    - *staff, through regular briefings*
    - *learners, through assemblies/lessons*
    - *parents/carers, through newsletters, school social media, website*
    - *governors, through regular safeguarding updates*
    - *local authority/external agencies, as relevant*

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


Online Safety Incident Flowchart
Unsuitable materials or activity
Illegal materials or activities found or suspected
Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team
If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions[1].
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
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 professional body.

School actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows: (the school will need to agree upon its own responses and place the ticks in the relevant columns. They may also wish to add additional text to the column(s) on the left to clarify issues. Schools have found it useful to use the charts below at staff meetings/training sessions)

Responding to Learner Actions

Incidents	Refer to class teacher/tutor	Refer to Head of Year / Senior Leader	Refer to Headteacher	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/carers	Remove device/ network/internet access rights	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X	X	X		X			X
Attempting to access or accessing the school network, using another user's account (staff or 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			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			X			
Accidentally accessing offensive or pornographic material and failing to report the incident.	X	X				X			
Deliberately accessing or trying to access offensive or pornographic material.			X			X	X		X
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.									
Continued infringements of the above, following previous warnings or sanctions.			X						X

Responding to Staff Actions

Incidents	Refer to line manager	Refer to Headteacher/ Principal	Refer to local authority/MAT/HR	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
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
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	X		
Breaching copyright or licensing regulations.		X				X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.		X			X	X		
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		X						X
Using personal e-mail/social networking/messaging to carry out digital		X	X					X

communications with learners and parents/carers								
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail		X						X
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner		X				X		
Actions which could compromise the staff member's professional standing		X						X
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						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 and regularly taught in a variety of contexts.**
- **Lessons are matched to need; are age-related and build on prior learning**
- **Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes**
- **Learner need and progress are addressed through effective planning and assessment**
- **Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc**
- **it incorporates/makes use of relevant national initiatives and opportunities e.g. *Safer Internet Day* and *Anti-bullying week***
- **the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.**
- *learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school*
- *staff should act as good role models in their use of digital technologies the internet and mobile devices*
- *in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- *where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit*

- *it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need*
- **the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.**

Contribution of Learners

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

- *mechanisms to canvass learner feedback and opinion.*
- *appointment of anti-bullying ambassadors/care team)*
- *learners designing/updating acceptable use agreements*
- *contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.*

Staff/volunteers

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

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

Governors

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

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

A higher level of training will be made available to the Safeguarding Governor.

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 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).*

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 (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)*
- *younger learners will use child friendly/age-appropriate search engines*
- filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.
- *access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.*

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

Monitoring

The 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*

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.**

- 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
- The Network Manager 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

Mobile technologies

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[1]	Student owned	Staff owned	Visitor owned
Allowed in school	**Yes**	**Yes**	**Yes**	Yes- left in office	Yes	Yes
Full network access	Yes	Yes	Yes	No	Wifi linked	No
Internet only	-	-	-	-	-	-
No network access	-	-	-	Yes	Yes	Yes

School owned/provided devices:

- *are given to all staff who require them. Staff can access ipads/laptops. Senior staff will also have access to mobile phone provided by school*
- *They access the network onsite and remotely from anywhere with a wifi link.*
- *School devices should not be used for personal issues*
- *levels of access to networks is limites based on the staff members role*
- *management of devices/installation of apps/changing of settings/monitoring is controlled by the Network manager*
- *technical support is provided by the network manager. No unauthorised persons should be providing technical support for hardware or software*
- *filtering of devices is done through the Smoothwall system*

Personal devices

- *Personal devices can only be used by staff in areas where children are not present e.g staffroom, offices, classrooms after school etc. No pupils are allowed access to personal devices. If children bring mobile phones/technology to school they must hand it in at the office upon arrival and collect at the end of the day. The only exceptions are those*

[1] Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

with medical conditions such as diabetes where the technology is used to support the medical condition eg insulin pumps. In this case parents and children will agree to use the technology only for the medical purposes required.

Social media

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/ middle leaders
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- 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

Monitoring of public social media

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

Digital and video images

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

- **the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.**
- **when using digital images, staff will inform and educate 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**
- **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**

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 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. For further information refer to the school's data Protection Policy.

School Online Safety Policy Template Appendices

Appendices

IT ACCEPTABLE USE POLICY

For Children

At Skelton Primary School we do all that we can to keep pupils safe when using any of our IT systems, but it is expected that you will also help us by making sure that you follow all of the advice given, including staying safe when using the Internet. This way we can work together to keep you and our computer systems safe and enable you to get the most out of IT to help you with your learning.

So that we can make our IT systems as safe and secure as possible, a list of rules must be followed. Keeping to these rules will ensure that we can continue to provide quality IT facilities that you, our children deserve.

S.P.S. will ensure good access to IT to enhance learning and in return, expect the children to be responsible users as outlined below:

RULES FOR SAFE & RESPONSIBLE USE OF IT

For my own personal safety: I know that irresponsible use of IT systems may result in the loss of computer, printing, emails and/ or internet access either on a temporary or permanent basis and that punishment may follow.

I will:

- Log onto all school computer systems using only my own username and password and I will not share this information with anyone else.
- Only use school computer systems, e-mail and Internet access that are appropriate to my education.
- Only use IT equipment that is supplied to me by the school.
- Access the school's wireless system with school IT equipment only.
- Use all media responsibly, carefully and politely and will not write anything that I would not put in a letter or note, as it can easily be copied, forwarded, or sent to the wrong person by mistake and I know that I am responsible for all e-mails I send and contacts I make.
- Treat the equipment with respect, as I know that any deliberate damaging of equipment will not be tolerated, will be charged for and a punishment given.
- Take sound recordings, pictures or videos on school equipment only and then only with permission from a teacher or a member of staff.
- Only make sound recordings, pictures or videos, if the person involved gives their consent.
- Be aware of 'stranger danger' when I am communicating on line.
- Report to a teacher or member of staff any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I am on line.
- Be aware that when using the Internet to find information, that it may not be accurate or correct.

I will not:

- Post any of my personal details or images on a website, blog, or in an e-mail etc. unless authorised to do so by a teacher, or a member of staff.

- Send or try to look at, save, print, or show offensive messages or pictures on any of the school's IT systems. If any of these accidentally come on my screen, I will inform my teacher immediately.
- Access, move, delete or in any way change anyone else's work.
- Attempt to fix a problem myself, but will inform a teacher or member of staff if I find anything wrong with any IT equipment.
- Run any programs, games etc. on any of the school IT systems, from portable storage devices such as a USB pen, hard drive, MP3 player etc.
- Use or attempt to use a mobile phone whilst in the school.
- Use or try to use public chat rooms, blogs or social networking sites whilst in the school.
- Use or connect to any Bluetooth device on any school systems.
- Look or try to look at adult, racist, homophobic or other offensive or illegal material.
- Use IT systems for online bullying, racial or homophobic harassment or intimidation.
- Use social media in a way that will be offensive or threatening to others.

In circumstances where the school's IT systems have allegedly been used for storing text or images that are unauthorised or unlawful, or for criminal purposes, S.P.S. will exercise its right by electronic means to monitor the use of the school's IT systems. This includes the monitoring of documents, Internet use, the interception of e-mails and the deletion of inappropriate materials from our IT systems.

Please take time to discuss the above document with your child and then complete, sign and return to your child's class teacher

Child: ……Class:……

Pupil's Agreement

I have read and understood Skelton Primary School's IT Acceptable Use Policy for Children. I will use the IT systems and Internet in a responsible way and obey these rules at all times. I understand that I will be expected to pay for any damage I cause to equipment.

Signature of child: ……Date: ……..

Skelton Primary School Media Consent Form

<table>
<tr><td colspan="5">Your Consent Preferences
This form has been written to give you choice and control over how our school uses some of your personal data.

You may withdraw these consent preferences at any time. Further information about how to do this can be found below.</td></tr>
<tr><td rowspan="2">Non-Essential Communications
The school will want to contact you to tell you about school events, news, and general updates. Please state if you would like to receive these communications. Eg Friday Flyer etc

If so, please tick which apply.</td><td colspan="2">YES</td><td colspan="2">NO</td></tr>
<tr><td>HARD COPY</td><td>EMAIL</td><td></td><td></td></tr>
<tr><td>If you require communication by email please provide email details:</td><td colspan="4"></td></tr>
<tr><td colspan="5">School’s use of images:

In Skelton Primary School, digital media is vital to record the child’s learning journey and help celebrate their achievements.
If you wish to give consent to some, but not all of these areas, please tick those which you consent to.
Images may be used for:
○ Display
○ Evidencing key moments in learning
○ Group/ class photos
○ School’s online presence- Website, Blog, official School Facebook page, Friday Flyer
○ External media events- Press, TV, Radio

Skelton Primary School is keen to celebrate your children’s success with you but also recognises the risks of keeping children safe in an online world.
We will therefore reduce any risks by using as few identifiable factors as possible. Images may be uncaptioned or only use first names etc.</td></tr>
</table>

Photos and Videos **I consent to school using images and videos of my child to ensure the needs of the school and curriculum are met.**	**YES**	**NO**

Parent/Guardian Name:	Parent's Signature:
Pupil Name:	
Date:	

To withdraw or change your consent preferences please contact:

The office manager at school or office@skeltonprimaryschool.co.uk

To find out more about how our school uses your personal data then please see our privacy notice and e-safety policy which can be found on our website- www.skeltonprimaryschool.co.uk

Parent's Consent for Internet Access

I have read and understand Skelton Primary School's 'rules for safe and responsible use of IT and give permission for my son/daughter to access the Internet.

I understand that the school will take all reasonable precautions to ensure students cannot access inappropriate materials and I agree that the school cannot be held responsible for the nature or content of materials accessed through the Internet.

I agree that the school is not liable for any damages arising from use of the Internet facilities.

We will support the Academy approach to online Safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community.

I understand that we may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use
and will not be published on the internet including social networking sites

I understand that I will be charged if my son/daughter damages any IT equipment.

Signature of Parent/Carer: ……

Please print name: ……Date……

IT Agreed Usage Policy

for Staff

As part of our commitment to provide the best Teaching and Learning opportunity for our children, particularly when using IT, a wide range of facilities are made available to staff to assist them in delivering their Teaching through IT. It is however, necessary that we ask all our staff to use our computer systems in a safe and responsible manner.

The computer systems owned by Skelton Primary School offers safe, secure and reliable access to a number of services:-

- E-mail
- Data storage
- Internet access
- Printing, scanning & copying
- A Virtual Learning Environment
- A wide range of educational & office software

All of these facilities are available for our staff to utilise, but in order to make them safe, secure and reliable we have a number of measures in place, such as: -

- Secure Data Storage & Backup Systems
- Logon Usernames and Passwords
- Anti-Virus Software
- Web Filtering
- Firewall

It is staff's responsibility to ensure that electronic platforms, such as S.P.S logins, CPOMs and email accounts, are correctly logged out when not in use to ensure the safety of both pupils and staff is maintained.

To maintain a safe and secure IT environment, an Agreed Usage Policy must be enforced. Adherence to this policy will ensure that we can continue to provide the level of service that our students deserve and that our staff have come to expect.

All Staff who intend to use the Academy IT Network and access any of the Academy systems, i.e. SIMS, E-mail, VLE, Printing etc. must comply with this IT Acceptable Use Policy (AUP) and sign an AUP Consent Form.

Unlawful and Illegal Use

The Skelton Primary School IT Network (LAN) and associated services may be used for lawful purposes only.

As a user of the Academy IT systems you agree not to send or receive materials or data that is n violation of any law or regulation which :

- constitutes harassment
- is defamatory, abusive, indecent or obscene
- is in breach of confidence, privacy or data protection
- is in breach of any third party intellectual property rights (including copyright)
- is in breach of any other rights or has any fraudulent purpose of effect

You are prohibited from storing, distributing or transmitting or permitting the storage distribution, or transmission (whether intentionally or otherwise) of, any unlawful material through the school IT systems. Examples of unlawful material include but are not restricted to:

- Direct threats of physical harm
- Hard core and child pornography
- Copyrighted, trademarked and other proprietary material used without proper authorisation
- Any other material that may be considered offensive

Examples of S.P.S. systems & storage: -

- Instant messaging or chat
- Local machine hard drive
- Users' home directory o Public directory
- Staff directory
- E-mail

Violations of Systems or Network Security

Any violations of the computer systems or network security are prohibited, and may result in the 'User' facing criminal and civil liability. S.P.S. will investigate such incidents, and will inform and co-operate with the relevant law enforcement agencies if a criminal violation is suspected.

Computer Usage

When using any of the school computer systems and associated equipment, i.e. Computers, Email, Printing, Online Testing etc. the following rules apply: -

- All of the Academy systems are to be used for work that is in connection with your professional role within the Academy
- All IT systems should only be accessed using your own authorised Username and Password
- Your Username and Password should not be shared with anyone else, **students in particular**
  - It is staff's responsibility to ensure that electronic platforms, such as S.P.S logins, CPOMs and email accounts, are correctly logged out when not in use to ensure the safety of both pupils and staff is maintained.
- As regards security, your Passwords should be given the same consideration as your Bank Card number
- Under no circumstances should you use anyone else's Username and Password to access any of the Academy systems
- Should you suspect that anyone has discovered any of your passwords, they should immediately be changed and the details reported to the IT Technician. It is recommended that in order to keep your information safe and secure, that you change your passwords regularly (advice on this can be obtained from the IT Technician.
- In order to protect your information, and the school data from unauthorised access, it is expected that when using any of the school systems, you will lock your computer when you are not in attendance.
- All work is to be saved in your Home directory, or in a designated folder on Public or Staff directories, or in the case of Administration Staff, the Common directory
- Although the Academy considers the use of e-mail as an informal method of communication, it is still requisite that the same professional conduct applies to its use, as that of formal communication, i.e. letters, memos etc.
- Staff are responsible for all e-mails that they send, and for any contacts that are made as a result of this, which may result in e-mails being received
- You may not send e-mail to any user who does not wish to receive it, or send emails which could be considered as offensive
- When e-mailing a child you should always copy in your line manager, or another member of staff, to ensure that contact is clear and open
- The posting of anonymous messages and forwarding of emails that are not work related is forbidden
- Use for advertising, gambling, political purposes, personal or financial gain is strictly prohibited
- Accessing, reproducing, sending, posting or distributing anything that is bullying, racist, pornographic, or offensive in nature is strictly prohibited
- Use for cyber bullying, racial harassment or intimidation is strictly forbidden
- The use of Blogs is 'only' allowed on those sites approved by S.P.S.
- Use of chat or instant messaging is permitted but 'only' through those provided by the Academy (Teams)
- The sending of text or picture messages to mobile phones from the Internet is not allowed unless this is work-related
- You must not give out any of your personal details to children, including mobile phone or home phone numbers, such communication as may be required can be made using a mobile phone provided by school.
- In order to protect yourself, you should never initiate or allow any contact with children through social network sites or other such medium from outside school
- Ensure that personal social networking sites are set at private and children are never listed as approved contacts and use social media in line with the Social Media Policy and Guidelines
- If you do choose to operate a social networking site or blog, any activity that may bring the school into disrepute, will be addressed through disciplinary action

- You should not access any chidlren's social network site
- All software for use on the system must be approved by the IT Team and can only be installed by an IT Technician. Details concerning this can be obtained by contacting the IT Technician.
- Installation of programs and games can only be carried out by a member of the IT Team
- Copying of data that is not for use in connection with your professional role within school (including Images, Videos, Music, or Text) is not allowed
- You may not post or otherwise distribute or permit the posting, uploading or distribution (whether intentionally or otherwise) of copyrighted material on any of the school systems, without written consent from the copyright holder. These include but are not restricted to, Music, Videos, Images, or Text
- You are not allowed to delete, move or in any way modify the work of others, without their express permission
- All Internet access must go through Academy systems, which includes the use of personal laptops, tablets etc. Should you require Internet access on a personal device, please contact a member of the IT Team.
- Any activity that may cause damage to the computer systems such as, physical abuse, computer hacking or the deployment of a computer virus, or other malicious software is strictly forbidden
- Any misuse or damage to computers should be reported to the IT technician
- Any faulty computer hardware should be reported to the IT technician
- All portable IT equipment (such as a laptop or mobile phone) should be stored with appropriate security precautions and such items should not be left in an unattended vehicle

Violations may include, but are not limited to the following: -

- Unauthorised access to or use of data, software or networks, including any attempt to probe, scan or test for vulnerability of the network
- Unauthorised monitoring of data or traffic on the network, without express permission of the S.P.S. SLT
- Interfering with any user, or the network and deliberate attempts to overload the system
- Irresponsible use of passwords, as these should be changed on a regular basis (and as mentioned above) under no circumstances shared with anyone, staff or child

Filming and Photography

- The taking of photographs or filming of children, is only allowed where permission has been given by receipt of a signed 'Authorisation Form' from a parent or carer, (Office will have details concerning this) and then only if the children concerned give their consent
- Filming and the taking of photographs of children with your own personal mobile phone or camera is forbidden, this should only be undertaken using equipment specifically provided by the Academy for this purpose
- Photographs or videos involving children can only be used in connection with Teaching and Learning within S.P.S.
  Photographs and videos of children should be edited/ dated/ stored in a Staff shared area wherever possible, and if not possible be clearly marked as to what purpose they are being used, in line with school policy
- Photographs and videos of children should be deleted after use, or if they need to be archived for any purpose, be placed in a shared staff area, in line with school policy

Disciplinary and Related Action

Failure to comply with any of the rules as stated within the 'IT Agreed Usage Policy for staff' may result in disciplinary action being taken. In the case of any suspected abuse of the school E-mail system, Internet access and General access, the user will have their account suspended pending an investigation into such abuse. The above actions will be mandatory and any other sanctions that the management see fit to impose will also apply. These will be dependent upon the nature and severity of the offence and will not exclude reporting to relevant authorities should there be any criminal implications.

Skelton Primary School wishes to promote the highest standards in relation to good practice and security in the use of information technology. Consequently it expects and supports the integrity of its users. In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.

Examples: -

- Criminal Acts – for example in relation to child pornography
- Visiting pornographic sites (adult top shelf materials)
- Causing offence to religious groups or racial incitement
- Chat rooms – sexual discourse, arrangements for sexual activity
- Software media counterfeiting or illegitimate distribution of copied software

Decision to Advise the Police for Criminal Investigation

On the facts that are immediately available, a decision will be taken whether to refer the matter to the Police for criminal investigation. This does not preclude the matter being referred to the Police at any later stage when a formal investigation has been undertaken.

Where Skelton Primary School are approached by an officer from the Local Authority or any public body asking to provide evidence or monitoring of a suspected site, the following rules will apply.

Disclaimer

SPS will endeavour, wherever possible, to provide a safe and secure environment for its users. However, users must be aware that we cannot guarantee complete safety from inappropriate material. Users must be aware of sites being accessed and report any inappropriate material immediately to the IT Support

Staff

IT Agreed Usage Policy Consent Form

By signing this consent form you are allowed to access all of the school's IT systems, including the Data Network, Internet, E-mail, Printing and our Virtual Learning Environment. All of our IT systems are here to assist our staff to optimise their use of IT in supporting and delivering Teaching and Learning to the highest standards.

Declaration

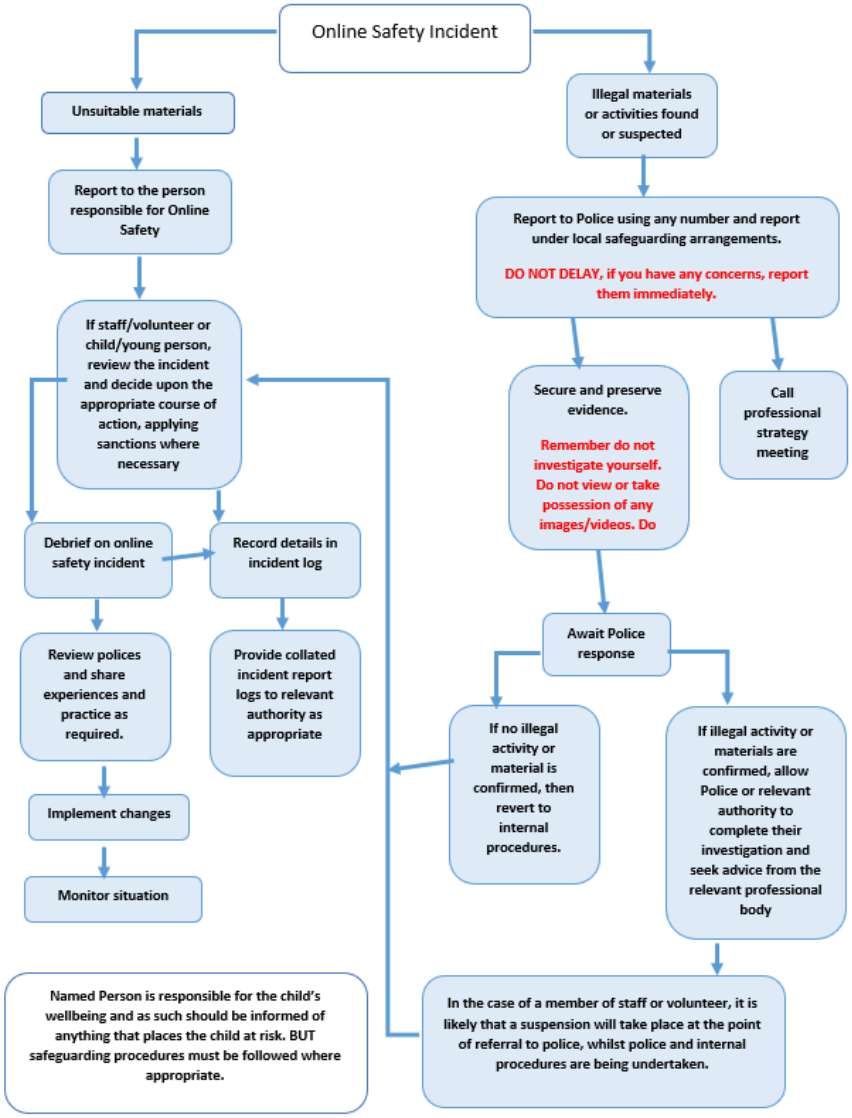
I have read the Staff IT Agreed Usage Policy and I agree to use the school's computer systems in accordance with these rules. I understand that if I breach any of these rules, I will be subject to disciplinary action.

Date……..

Print Name……

Signed……..

Responding to incidents of misuse – flow chart



Links to other organisations or documents

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

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Revenge Porn Helpline - https://revengepornhelpline.org.uk/
Internet Watch Foundation - https://www.iwf.org.uk/
Report Harmful Content - https://reportharmfulcontent.com/
Harmful Sexual Support Service

CEOP

CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources
Kent – Online Safety Resources page
INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Tools for Schools / other organisations

Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
360Data – online data protection self-review tool: www.360data.org.uk
SWGfL Test filtering - http://testfiltering.com/
UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework
SWGfL 360 Groups – online safety self review tool for organisations working with children
SWGfL 360 Early Years - online safety self review tool for early years organisations

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/
SELMA – Hacking Hate - https://selma.swgfl.co.uk
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
DfE - Cyberbullying guidance -
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – Cyberbullying guidance and practical PSHE toolkit:
http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit

Childnet – Project deSHAME – Online Sexual Harrassment
UKSIC – Sexting Resources
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
Ditch the Label – Online Bullying Charity
Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking
UKSIC - Safety Features on Social Networks
Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Evolve - https://projectevolve.co.uk
UKCCIS – Education for a connected world framework
Department for Education: Teaching Online Safety in Schools

Teach Today – www.teachtoday.eu/
Insafe - Education Resources

Data Protection

360data - free questionnaire and data protection self review tool

ICO Guides for Organisations

IRMS - Records Management Toolkit for Schools

ICO Guidance on taking photos in schools

Professional Standards/Staff Training

DfE – Keeping Children Safe in Education
DfE - Safer Working Practice for Adults who Work with Children and Young People
Childnet – School Pack for Online Safety Awareness
UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support/Cyber-security

UKSIC – Appropriate Filtering and Monitoring
SWGfL Safety & Security Resources
Somerset - Questions for Technical Support
SWGfL - Cyber Security in Schools.
NCA – Guide to the Computer Misuse Act
NEN – Advice and Guidance Notes

Working with parents and carers

SWGfL – Online Safety Guidance for Parents & Carers
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops/education
Internet Matters

Prevent

Prevent Duty Guidance
Prevent for schools – teaching resources
Childnet – Trust Me

Research

Ofcom –Media Literacy Research
Ofsted: Review of sexual abuse in schools and colleges

Further links can be found at the end of the UKCIS Education for a Connected World Framework

Glossary of Terms

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

WAP	Wireless Application Protocol