The Federation of

Stoke Hill Schools

Online Safety Policy

Including IT Acceptable Use policy for Staff, Governors and Pupils

Approved by:	Teaching and Learning Committee
Last reviewed on:	**27.04.23**
Next review due by:	April 2024

CONTENTS

Online Safety Policy

1 Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupilslearn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This Online -safety policy helps to ensure safe and appropriate use. The development and implementation of such a strategy involves all the stakeholders in a child's education from the head teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this Online safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which

they may be exposed, so that they have the confidence and skills to face and deal with these risks.
The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The Online-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

2 Development / Monitoring / Review of this Policy

This Online-safety policy has been developed by:

- *Senior Leaders*
- *Teachers*
- *Support Staff*
- *ICT Technical staff*
- *Governors*

Consultation with the whole school community has taken place through the following:

- *Staff meetings*
- *Governors meeting / sub committee meeting*

The school will monitor the impact of the policy using:

- *Logs of reported incidents - CPOMS*
- *SCOMIS monitor internet activity (including sites visited)*
- *Internal monitoring data for network activity*
- *Surveys / questionnaires of*
- *students / pupils*
- *parents / carers*
- *staff*

3 Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The 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.

4 Roles and Responsibilities

The following section outlines the roles and responsibilities for Online-safety of individuals and groups within the school:

4.1 Governors:

Governors are responsible for the approval of the Online -Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Teaching and Learning Committee receiving regular information about Online-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online -Safety / Safeguarding Governor The role of the Online -Safety Governor will include:

- *regular meetings with the Designated Safeguarding Leaders – Heads Of School*
- *regular monitoring of e-safety incident logs*
- *regular monitoring of filtering / change control logs*
- *reporting to relevant Governors committee / meeting*

4.2 Head teacher and Senior Leaders:

The Head teacher is responsible for ensuring the safety (including Online Safety) of members of the school community.

- The Head teacher / Senior Leaders are responsible for ensuring that staff receive suitable CPD to enable them to carry out their Online-safety roles and to train other colleagues, as relevant
- The Senior Leadership Team will receive regular monitoring reports from the ICT technician.
- **The Headteacher and Leadership Team should be aware of the procedures to be followed in the event of a serious Online safety allegation being made against a member of staff.** (see SWGfL flow chart on dealing with Online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures)
- The Headteacher/ Senior Leaders are responsible for ensuring that relevant staff receive suitable training to enable them to carry out their Online safety roles and to train other colleagues, as relevant.
- The Headteacher // Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- The Senior Leadership Team / Senior Management Team will receive regular monitoring reports.
- Termly advice to parents/carers/grandparents/relatives around E-safety and recommended usage of ICT at home.

- Online Safety Coordinator / Officer:

(It is strongly recommended that each school should have a named member of staff with a day to day responsibility for Online Safety, For the Federation of Stoke Hill Schools, this role is carried out by Claire McKimm and Jamie Sullivan

- lead the Online Safety Group
- takes day to day responsibility for Online safety issues and has a leading role in establishing and reviewing the school Online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an Online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of Online safety incidents and creates a log of incidents to inform future Online safety developments, /
- meets regularly with Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

4.3 Network Manager / Technical staff:

Scomis is responsible for ensuring:

- **that the school's ICT infrastructure is secure and is not open to misuse or malicious attack**
- **that the school meets the Online-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online - Safety Policy and guidance**
- **that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed**
- SWGfL is informed of issues relating to the filtering applied by the Grid
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix "Filtering Policy Template" for good practice document)
- that he / she keeps up to date with Online-safety technical information in order to effectively carry out their Online -safety role and to inform and update others as relevant
- that the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher / Senior Leader ICT Co-ordinator
- that monitoring software / systems are implemented and updated as agreed in school policies

4.4 Teaching and Support Staff

are responsible for ensuring that:

- **they have an up to date awareness of Online-safety matters and of the current school Online -safety policy and practices**
- **they have read, understood and signed the school Staff Acceptable Use protocol**
- **they report any suspected misuse or problem to the Head of School or Executive Headteacher / Leadership Team for investigation**
- **digital communications with pupils/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 school activities
- pupils understand and follow the school Online -safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of Online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

4.5 Designated Safeguarding Lead

should be trained in Online-safety issues and be aware of the potential for serious child protection/Safeguarding issues to arise from:

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

Note: It is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop. Therefore at Stoke Hill we have decided to combine the role of Safeguarding Lead and Online Officer.

4.6 Teaching and Learning Committee

Members of the Teaching and Learning Committee; will assist the Head teacher with:

- mapping and reviewing the Online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the Online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

4.7 Pupils in KS2:

- **are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which the Parents/Carers are expected to sign on behalf of the pupil before being given access to school systems.**

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- 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

4.8 Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through newsletters, letters, website and information about national / local Online-safety campaigns / literature.

Parents and carers will be encouraged to support the school in promoting good Online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line student / pupil records and applications such as Seesaw
- their children's personal devices in the school (where this is allowed)

Parents and carers will be responsible for:

- endorsing (by signature) the acceptable use of internet / ICT for their children in the Infant and Nursery school.
- At KS2 the Parent/Carer is responsible for ensuring their child understands and signs the Pupil Acceptable Use Policy

4.9 Community Users

Community Users who access school ICT systems / website as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

5 Policy Statements

5.1 Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

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 programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key Online -safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. (Nb. additional duties for schools / academies under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.)
- Pupils should be helped to understand the need for the pupil safety and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Rules for use of ICT systems / internet will be posted in all classrooms.
- Staff should act as good role models in their use of ICT, the internet and mobile devices

5.2 Education – parents / carers

Many parents and carers have only a limited understanding of Online e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).
The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site.
- Parents evenings

5.3 Education - Extended Schools

The school will signpost family learning courses in ICT, media literacy and Online-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

5.4 Education & Training – Staff

- It is essential that all staff receive Online safety training and understand their responsibilities, as outlined in this policy.
- An audit of the Online safety training needs of all staff will be carried out regularly. Online Safety BOOST includes unlimited Online webinar training for all, or nominated, staff (https://boost.swgfl.org.uk/)
- All new staff should receive Online safety training as part of their induction programme, ensuring that they fully understand the school / academy Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify Online safety as a training need within the performance management process.
- The Online Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

5.5 Training – Governors

Teaching and Learning Committee Governors should take part in annual e-safety training / awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / SWGfL or other relevant organisation.
- Participation in school training / information sessions for staff or parents

5.6 Technical – infrastructure / equipment, filtering and monitoring

The school will be 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. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their Online-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the Online-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems.
- All pupils will be provided with an individual username and password for use with Chromebooks

- The “master / administrator” passwords for the school ICT system are held in the school safe and a copy is held by administrative staff.
- The Computing Lead is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. (the school will need to decide on the merits of external / internal provision of the filtering service – see appendix). There is a clear process in place to deal with requests for filtering changes (see appendix for more details)
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet. Nb. additional duties for schools / academies under the Counter Terrorism and Securities Act 2015 which requires schools / academies to ensure that children are safe from terrorist and extremist material on the internet. (see appendix for information on “appropriate filtering”).
- The school maintains and supports the managed filtering service provided by SWGfL –
- In the event of the need to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head teacher. Office staff (TW and LL) hold the password and access for managing the system.
- Any filtering issues should be reported immediately to SWGfL.

• Remote management tools are used by Scomis to manage problems and carry out updates.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, visitors) onto the school system by logging on as a pupil according to the year group they are working within. In the case of long term placements e.g. SCITT students then a log on will be provided by the ICT SIP Team, in accordance with the staff protocol.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school. (See staff protocol)
- The school infrastructure and individual workstations are protected by up to date virus software.
- All laptops are password protected.

6 Curriculum

Online-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- At KS2 Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

7 Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. Such images may provide avenues for cyberbullying to take place.. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- **In KS2 When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.**

Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

Any photos taken to identify H&S risks/maintenance needs need to be free of images of children

- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils names will not be used anywhere on a website without prior parental/carer consent.
- Written permission from parents or carers will be obtained before photographs of pupils / pupil's work are published on the school website as part of the consent form for pupil images and internet use signed by parents or carers.

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 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 students / pupils in the digital / video images.

8 Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (see Privacy Notice section in the appendix)
- It has a Data Protection Policy (see appendix for template policy)
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

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.**
- **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 and secure password protected devices.**

When data is stored on any portable computer system, USB stick or any other removable media:

- the data must be stored on the Google Drive
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

9 Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at lunch times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓					✓		
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones			✓					✓
Use of hand held devices eg PDAs, PSPs	✓, but not in a teaching session.							✓
Use of personal email addresses in school, or on school network		✓						✓
Use of school email for personal emails	✓							✓
Use of chat rooms / facilities		✓						✓
Use of instant messaging		✓						✓
Use of social networking sites		✓						✓
Use of blogs		✓						✓

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

- **The official school email service may be regarded as safe and secure and is monitored.**
- **Users need to be aware that email communications may be monitored**
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.**

- **Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.** These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- *at KS2 and above will be provided with individual school email addresses for educational use.*
- Pupil should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Pupils are allowed to bring mobile phones to school for use before / after school, but they must remain in bags at all times whilst on school premises

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school / academy or local authority / academy group liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The Federation provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

Federation staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in Online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the Federation or local authority
- **Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information**

When official Federation social media accounts are established there should be:

- A process for approval by senior leaders

- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under Federation disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the Federation or impacts on the Federation, it must be made clear that the member of staff is not communicating on behalf of the Federation 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 Federation 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 Federation permits reasonable and appropriate access to private social media sites
- Monitoring of Public Social Media
- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the Federation
- The Federation should effectively respond to social media comments made by others according to a defined policy or process
- The Federation's use of social media for professional purposes will be checked regularly by the senior risk officer to ensure compliance with the Federation policies.

10 Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from Federation and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school /academy context, either because of the age of the users or the nature of those activities. The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				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 / academy				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)	x				
On-line gaming (non-educational)		x			
On-line gambling				x	
On-line shopping / commerce		x			
File sharing	x				
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting e.g. Youtube	X				

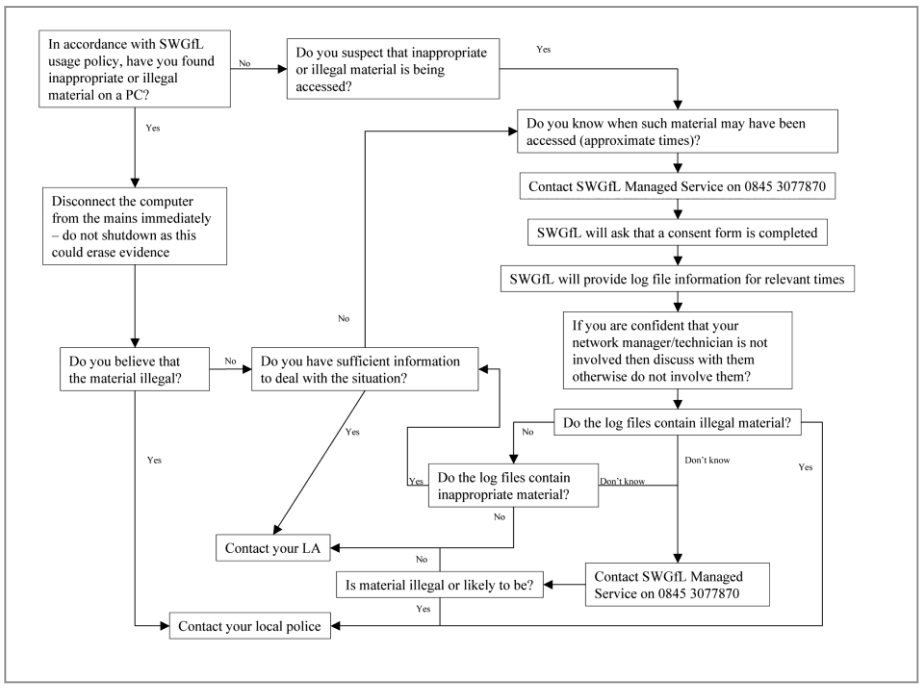
11 Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- **child sexual abuse images**
- **adult material which potentially breaches the Obscene Publications Act**
- **criminally racist material**
- **other criminal conduct, activity or materials**

the SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.aspshould be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

In the event of suspicion, all steps in this procedure should be followed:
Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise.
- Use the same computer for the duration of the procedure.

- It is important to ensure that the relevant staff should 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 (except in the case of images of child sexual abuse – see below)
- 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 / Academy Group or national / local organisation (as relevant).
- Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Federation Actions & Sanctions
It is more likely that the Federation 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

Pupils Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal	✓	N/A	✓	✓	✓				✓

Unauthorised use of non-educational sites during lessons	✓	N/A	✓		✓				✓
Unauthorised use of mobile phone / digital camera / other handheld device	✓	N/A	✓			✓			✓
Unauthorised use of social networking/ instant messaging / personal email	✓	N/A	✓			✓			✓
Unauthorised downloading or uploading of files	✓	N/A	✓		✓	✓			✓
Allowing others to access school network by sharing username and passwords	✓	N/A	✓						
Attempting to access or accessing the school network, using another student's / pupil's account	✓	N/A	✓						
Attempting to access or accessing the school network, using the account of a member of staff	✓	N/A	✓						
Corrupting or destroying the data of other users	✓	N/A	✓		✓	✓			✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	N/A	✓						✓
Continued infringements of the above, following previous warnings or sanctions	✓	N/A	✓						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	N/A	✓						✓
Using proxy sites or other means to subvert the school's filtering system	✓	N/A	✓						
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	N/A	✓		✓	✓		✓	
Deliberately accessing or trying to access offensive or pornographic material	✓	N/A	✓		✓	✓			✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	N/A	✓						

Staff Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	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).		✓	✓	✓	✓		✓	✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		✓						
Unauthorised downloading or uploading of files		✓			✓	✓		
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		✓			✓		✓	
Careless use of personal data eg holding or transferring data in an insecure manner	✓	✓				✓		
Deliberate actions to breach data protection or network security rules		✓	✓	✓	✓		✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓	✓	✓	✓		✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓	✓				✓	✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		✓	✓			✓		
Actions which could compromise the staff member's professional standing		✓	✓	✓		✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓	✓			✓		✓
Using proxy sites or other means to subvert the school's filtering system		✓			✓	✓		
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓			✓	✓		

Deliberately accessing or trying to access offensive or pornographic material		✓	✓		✓	✓	✓	✓
Breaching copyright or licensing regulations	✓	✓				✓		
Continued infringements of the above, following previous warnings or sanctions		✓	✓					✓

12 Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online Safety Policy Template and of the 360 degree safe Online Safety Self Review Tool:

- Members of the SWGfL Online Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

Date on which policy was approved: Reviewed by T & L June 2021
This policy will be reviewed annually on (date): November 2022

Infant School Pupil Acceptable Use Agreement

I understand that I must use school computers in a responsible way, so there is no risk to my safety, other children's safety, or to the computers.

For my own personal safety:

- I understand that the school will always check how I use a computer.
- I will keep my usernames and passwords safe – I will not share it or try to use anyone else's username and password.
- I will not tell anyone information about me, or anyone else, when I'm online.
- I will tell an adult anything that worries or upsets me online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school devices are for learning - I will not use them for anything else unless I am told to.

I will act as I expect others to act toward me:

- I will respect others' work and will not open, change or delete it without their permission.
- I will be polite and responsible when I communicate with others online.
- I will not take pictures of anyone unless I am told to.

I recognise that the school has a responsibility to keep IT resources safe and protected for all:

- I will not try to open or find anything I shouldn't or anything that could upset others.
- I will tell a grown up straight away if any computers get broken.

I understand that I am responsible for my actions, both in and out of school:

- I understand that I should stick to these rules when I am out of school as well, to keep myself and others safe.
- I know that if I break the rules, I might not be able to use the computers and my parents may be contacted.

Junior School Pupil Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my usernames and passwords safe and secure – I will not share it or try to use any other person's username and password.
- I will not disclose or share personal information about myself or others when online
- I will tell an adult if anything I see online worries or upsets me.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school devices are for learning - I will not use them for other things unless I have permission.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or change any other user's files, without their permission.
- I will be polite and responsible when I communicate with others
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to keep IT resources safe and protected for all:

- I will not try to upload, download or access any materials which are inappropriate or may upset others.
- I will immediately report any damage or faults to equipment or software.
- I will not change computer settings.

I understand that I am responsible for my actions, both in and out of school:

- I understand that I should stick to these rules when I am out of school as well to keep myself and others safe.
- I know that if I break the rules I might not be able to use the computers and my parents may be contacted.

Staff, Volunteer and Governor Acceptable Use Policy Agreement

School Policy

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

This acceptable use policy is intended to ensure:

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

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

Acceptable Use Policy Agreement

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

For my professional and personal safety:

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

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

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

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

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school's ICT systems
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

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

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

Staff/Volunteer Name: .....

Signed: .....

Date: .....