School Online Safety Policy

Introduction

The following were consulted in the production of this policy:

- Governors
- Teaching Staff and Support Staff
- Pupils
- Parents

The online safety policy is to be reviewed annually.

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 students learn 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. Our school online safety policy is intended to help to ensure safe and appropriate use.

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 school recognises that 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
- Online-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, Inclusion, 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 students' 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 will endeavour to provide the necessary safeguards to help ensure that such risks are well managed and reduced. This online safety policy 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.

Development / Monitoring / Review of this Policy

This online safety policy has been developed by a working committee made up of:

- *School ICT Coordinators / Online Safety Leads – Jayne Rochford-Smith & Tilly Butter*
- *Teacher Tilly Butter and SLT Jayne Rochford-Smith*
- *ICT Technical staff / Network managers – Moore Stephens IT Solutions / Computeam LTD*
- *Governor – Pete Rogers*

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

- *Staff meetings*
- *School / Student / Pupil Council/ Pupil Voice*
- *INSET days*
- *Governors meeting / sub committee meeting*
- *Parents evening / Workshops*
- *School website / newsletters*

Schedule for Development / Monitoring / Review

The school's online safety policy was originally approved by ICT committee, Governors and Headteacher on:	9th December 2013
The implementation of this online safety policy will be monitored by the:	*ICT Co-ordinator*
Monitoring will take place at regular intervals:	*yearly*
The Governing Body / Governors Sub Committee 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:	*yearly*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the	*July 2020*

technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*Ben Ford: MAT IT Manager;* *Sarah Mellor: MAT Safeguarding officer* *LA Safeguarding Officer;* *Police Commissioner's Office*

The school will monitor the impact of the policy using:

- *Log files of reported online safety incidents on the school's CPOMS system*
- *Surveys / questionnaires of*
  - *pupils (eg Ofsted "Tell-us" survey / CEOP ThinkUknow survey)*
  - parents / carers
  - staff

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 digital technology systems, both in and out of the school.

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

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

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.

Roles and Responsibilities

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

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 *Governors* receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of *ICT Governor* **Pete Rogers**. The role of the ICT Governor will include:

- *regular meetings with the ICT Co-ordinator/Online Safety Lead/s*
- *regular monitoring of* online *safety incident logs (CPOMS system)*
- *regular monitoring of filtering / change control logs*

- *reporting to relevant Governors meeting*

Headteacher / Senior Leadership Team (SLT):

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- The Headteacher and (at least) another member of the SLT should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher / SLT are responsible for ensuring that the Online Safety Lead/s and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher / SLT 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 will receive regular monitoring reports from the Online Safety Lead/s.

ICT Coordinator / Online Safety Lead/s :

- leads 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 / MAT / 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 (on CPOMS system).
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant Governor Committee meeting.
- reports regularly to Senior Leadership Team.

Technical staff / Network Manager:

The Technical Staff / Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure & is not open to misuse or malicious attack.
- that the school meets required online safety technical requirements and any Local Authority / MAT / other relevant body Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.

- that the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leadership team / Online Safety Lead for investigation / action / sanction.
- that monitoring software /systems are implemented and updated as agreed in school policies.

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 Policy / Agreement (AUP)
- they report any suspected misuse or problem to the ICT Co-ordinator or member of SLT
- digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) 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 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
- it should be noted that where visiting staff are permitted to use the internet via the school's wifi network – they are enabled access to a "guest" network, totally separate from the school's main wifi network. This guest network is subject to the same filtering as the school wifi network.

Designated person for child protection / Child Protection Officer

should be trained in online safety issues and be aware of the potential for serious child protection 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
- online-bullying

Pupils :

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy. All pupils will be expected to understand acceptable use rules and KS2 children will be expected to sign these before being given access to school systems. Parents will also be asked to sign this contract.
- 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 online-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.

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 create opportunities to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local online safety campaigns / literature. Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy
- accessing the school website / VLE / on-line pupil records in accordance with the relevant school Acceptable Use Policy.
- abiding by the school's mobile phone use policy, which can be found on the school's website.

Community Users

Community Users who access school ICT systems / website / VLE as part of the Extended School provision will be expected to sign an AUP before being provided with access to school systems. This includes all students on placement at the school.

Policy Statements

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 online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online 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 curriculum should be provided as part of ICT / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and class-time 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 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 pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in 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 (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove 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.

Education – parents / carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's 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.

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

- Letters, newsletters, web site
- Parents / Carers evenings
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education - Extended Schools

The school will offer online safety training so that parents/carers and where appropriate, members of the wider community can together gain a better understanding of these issues. 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.

Education & Training – Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- 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 Lead/s will receive regular updates through attendance at external training events (eg from SWGfL / LA / MAT & 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 / meetings / INSET days.
- The Online Safety Lead/s will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / MAT / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

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 technical systems will be managed in ways that ensure that the school meets recommended technical requirements (these may be outlined in Local Authority / MAT / other relevant body policy and guidance)
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- While the school uses a VLE, all users (in KS2) will be provided with a username and secure password by (the ICT Coordinator/s) who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master / administrator" passwords for the school ICT systems, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe).
- The Network manager 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 is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering / monitoring 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.
- School / academy technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual 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, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff / pupils / parents / carers / community users) are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies

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

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

The school Acceptable Use Agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies. The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device**[i]	**Pupil owned**	**Staff owned**	**Visitor owned**
Allowed in school	*X*	*X*	*X*	*X*[1]	*X*[2]	*X*[2]
Full network access	*X*	*X*	*X*			
Internet only					*X*	*X*
No network access				*X*		

[1] Pupil Owned – mobile phones brought into school will be handed in to the class teacher and kept in the school office, to be returned at the end of the school day.
[2] Staff and Visitor Owned – mobile phones brought into school may only be used in designated spaces (Staffroom/SLT rooms).

See the School's Use of Mobile Phones Policy for more information.

Use of digital and video images

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. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

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 e.g. on social networking sites.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press
- Parents / carers are requested NOT to take videos and digital images of their children at school events.
- Staff and volunteers 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.

- 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.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data Protection

As of the 25th May 2018, the data protection arrangements for the UK changed following the introduction of European Union General Data Protection Regulations (GDPR).

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

The school must ensure that:

- It has a Data Protection Policy.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO).
- 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.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.

- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

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 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 personal data is stored on any portable computer system, memory stick or any other removable media:

- The device must be password protected.
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

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 certain 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	X						X	
Use of mobile phones in lessons				X				X
Use of mobile phones in social time	X*							X
Taking photos on mobile phones or cameras			X					X
Use of other mobile devices eg tablets, gaming devices	X						X	
Use of personal email in school, or on school network				X				X
Use of school email for personal emails				X				X
Use of messaging apps			X					X
Use of social media			X					X
Use of blogs	X						X	
Use of personal devices to access school's Wifi		X						X

* personal mobile phones are to be used in designated school areas during school hours/while children are in the school.

Parents, carers or casual visitors to the school will not be permitted to access the school's IT system or wifi network with their own devices, without specific permission granted in writing by the Headteacher.

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. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person, Headteacher – 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 students 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.
- Whole class or group email addresses will be used at KS1, while students / pupils at KS2 and above will be provided with individual school email addresses for educational use if necessary.
- Pupils 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.

Use of Social Media at school

The school has adopted the Bath and Wells Multi-Academy Trust's (BWMAT) policy on the use of social media. This can be found on the school's website on the Parent Info/Policies & Reports page.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. online-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 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 / or outside the school when using school equipment or systems. The school policy restricts usage as follows::

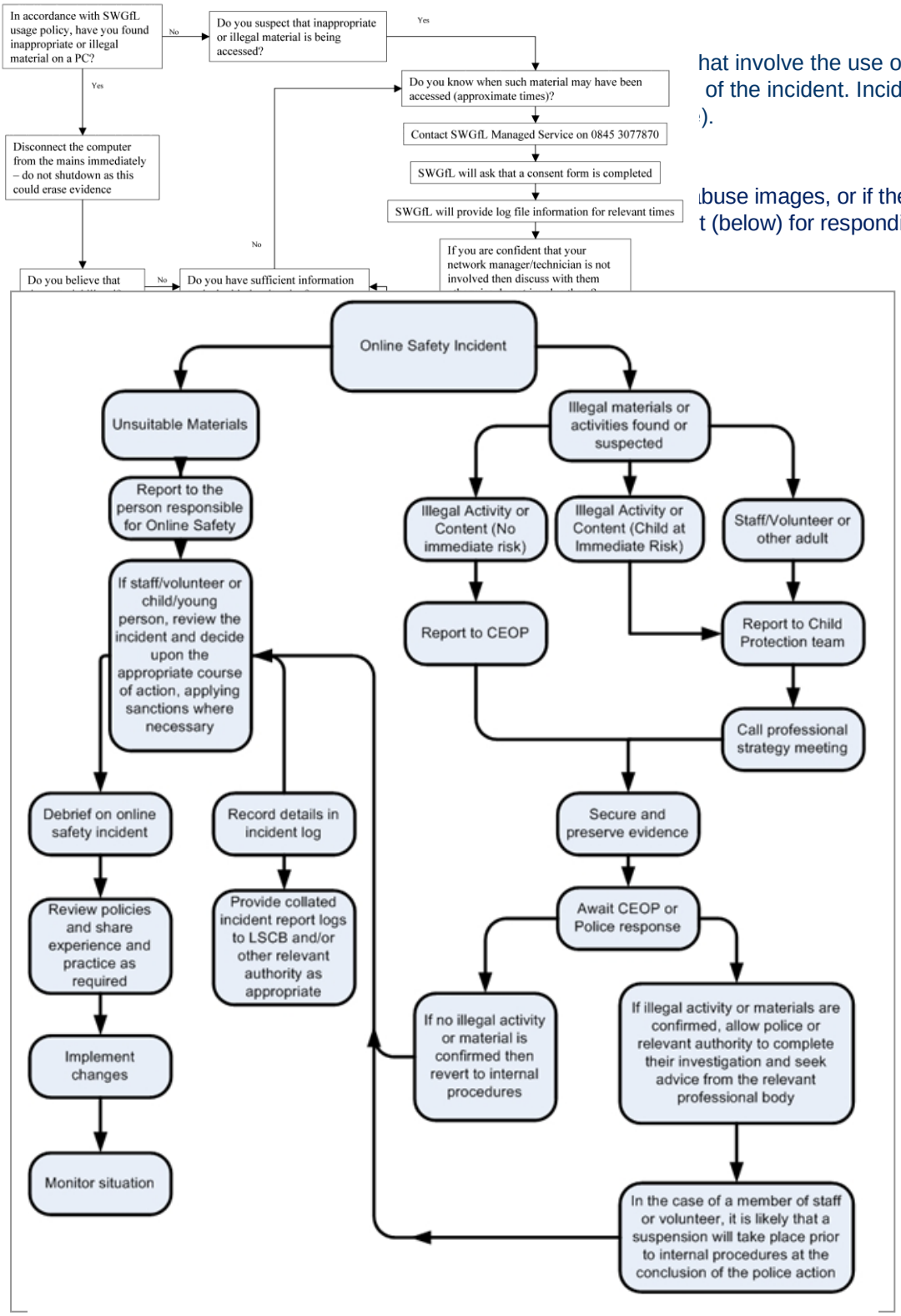
User Actions

		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	
	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					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		X	
File sharing				X		
Use of social media			X			
Use of messaging Apps			X			

Use of video broadcasting e.g. Youtube			X		

hat involve the use of online
of the incident. Incidents
).

buse images, or if there is any
t (below) for responding to



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff 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 / MAT.
- 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.

Pupil-related Incidents Actions / Sanctions

Incidents:	Refer to class teacher	Refer to Head of Key Stage	Refer to Headteacher	Refer to Police	Refer to technical staff for action	Inform parents / carers	Removal of network / internet access rights	Warning/education	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			X	X	X	X		X	
Unauthorised use of non-educational sites during lessons	X	X					X	X	
Unauthorised use of mobile phone / digital camera / other mobile device	X					X		X	
Unauthorised use of social media / messaging apps/ personal email	X	X				X	X	X	
Unauthorised downloading or uploading of files	X		X			X	X	X	
Allowing others to access school network by sharing username and passwords	X		X			X	X	X	
Attempting to access or accessing the school network, using another student's / pupil's account	X		X			X	X	X	
Attempting to access or accessing the school network, using the account of a member of staff	X		X			X	X	X	
Corrupting or destroying the data of other users	x		x			X	X	X	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X		X			X	X	X	
Continued infringements of the above, following previous warnings or sanctions			X			X			X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X		X			X	X	X	
Using proxy sites or other means to subvert the school's filtering system			X		X	X	X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X		X		X	X			
Deliberately accessing or trying to access offensive or pornographic material			X		X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X								

Staff-related Incidents Actions / Sanctions

Incidents: To be dealt with on a case-by-case basis in line with staff code of conduct policy.	Refer to line manager	Refer to Head teacher	Refer to LA/MAT/HR	Refer to Police	Refer to technical staff for action	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		X	
Unauthorised use of non-educational sites during lessons	X					X		
Unauthorised use of mobile phone / digital camera / other handheld device	X					X		
Unauthorised use of social networking / instant messaging / personal email	X	X				X		
Unauthorised downloading or uploading of files	X	X				X		
Allowing others to access school network by sharing username and passwords	X	X				X	X	
Attempting to access or accessing the school network, using another student's / pupil's account	X	X				X	X	
Attempting to access or accessing the school network, using the account of a member of staff	X	X				X	X	
Corrupting or destroying the data of other users	x	X					X	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X					X	
Continued infringements of the above, following previous warnings or sanctions		X						X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X				X	X	
Using proxy sites or other means to subvert the school's filtering system		X			X	X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X			
Deliberately accessing or trying to access offensive or pornographic material		X			X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X							

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: 12.07.19 …Pete Rogers…… Vice-chair of Governors

Policy review date: July 2020