Online Safety Policy

School Aim Statement:	Recognising its historic foundation, the school will preserve and develop its religious character in accordance with the principles of the Church of England and in partnership with the church at parish and diocesan level. The Christian Faith, and its practical expression, form a major part of the whole school ethos. The school aims to give children both knowledge and understanding of the Christian Faith while respecting and understanding other religions and cultures. The school aims to: - • ensure that all children receive their entitlement to a broad, balanced National Curriculum, encouraging them to have high expectations in all areas of the curriculum and to reach their full potential. • provide a secure and relaxed environment in which the children are encouraged to have a healthy lifestyle, to be tolerant and to grow in confidence and self-esteem. • ensure that pupils develop an open and enquiring mind and are encouraged to be creative, imaginative and inventive. • work in partnership with parents and the wider community.
Review History:	Review: June 2011, June 2014, September 2016 Next review: January 2019
Issue Date:	September 2016

Contents

1. Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by the Online safety committee made up of:

- Head teacher
- Online Safety Coordinator
- Staff – including Teachers, Teaching assistants
- Governors
- Parents and Carers

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

2. Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body	*September 2016*
The implementation of this Online Safety policy will be monitored by the:	*Online safety Committee*
Monitoring will take place at regular intervals:	*Annually*
The Performance and Standards 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:	*Termly as appropriate*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*September 2017*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Officer,* *LADO, Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- 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 the 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 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 (see School Behaviour Policy).

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 online safety roles and responsibilities 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 Governors Performance and standards Sub Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body (Yvette Grogan) has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator /
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs (with the head teacher)
- regular monitoring of filtering (with the head teacher)
- reporting to relevant Governors Performance and standards Committee

4.2 Head teacher and Senior Leaders:

- The Head teacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be shared with the Online Safety Co-ordinator.
- The Head teacher and Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in section 12.0 – "Responding to incidents of misuse"
- The Head teacher is responsible for ensuring that the Online Safety coordinator receives suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team will receive termly monitoring reports from the Online Safety Co-ordinator.

4.3 Online Safety Coordinator

- leads the Online Safety Group
- 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

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents

(in coordination with the Headteacher)

- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- meets termly with Online Safety Governor to discuss current issues, review incident logs and filtering
- attends Online safety committee meetings
- reports regularly to Senior Leadership Team

4.4 Network Manager

The Network Manager consists of the Headteacher, ICT/ Computing Coordinator and Technical Staff and is responsible for ensuring:

- that the school's 's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority Group / 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. (Appendix 5)
- the filtering policy is applied and updated on a regular basis and that its implementation is responsibility of WCC (see Appendix 5 "Technical Security Policy")
- 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, Online Safety Coordinator for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

4.5 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 Staff Acceptable Use Policy Agreement (AUP) Appendix 3
- they report any suspected misuse or problem to the Headteacher / Online Safety Coordinator for investigation / action / sanction
- all 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 activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- 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
- in lessons where internet use is pre-planned students / 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

4.6 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

4.7 Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives.

Members of the Online Safety Group will assist the Online Safety Coordinator with:

- the monitoring of the school Online Safety Policy.
- 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 pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

4.8 Pupils

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement (appendix 1)
- 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 policies on the use of mobile devices and digital cameras. They should also know and understand 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

4.9 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. The school will take every opportunity to help parents understand these issues through parents' evenings, 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

5.0 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 online safety 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 Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / 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.
- 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.

5.2 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 behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, website
- Parents / Carers evenings / sessions
- 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
- (See appendix 2)

5.3 Education & Training – Staff / Volunteers

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:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Coordinator will receive regular updates through attendance at external training events (eg from 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 meetings / INSET days.
- The Online Safety Coordinator 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
- Participation in school training / information sessions for staff or parents

The school is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. There will be regular reviews and audits of the safety and security of school technical systems

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the Admin officer 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 system, used by the Network Manager (or other person) must also be available to the Headteacher and kept in the school safe.
- WES ICT Development Service is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. Filtering changes are not requested.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet
- *The* school has provided differentiated user-level filtering (allowing different filtering levels for different groups of users – staff / pupils)
- School 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 head teacher.
- Appropriate security measures are in place, provided by WES ICT Development Service 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. This consists of time limited login details provided by the office staff.
- An agreed policy is in place (section 11) regarding the extent of personal use that users (staff / pupils) and their family members are allowed on school devices that may be used out of school.

6.0 Mobile Technologies (including BYOND)

Mobile technology devices are 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. 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 and pupils gives 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[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
No network access						

School owned / provided devices:

- **Class ipads** with filtered access to the internet via BYOND. These are for use solely on the school site. Personal use is not allowed. Filtered access is allowed to the internet. App installation and changing of settings only by approved members of staff. Technical support is provided by Warwickshire LA. Use of images in accordance with School guidance on the taking and storage of images. No access to cloud services.
- **Individual SEN pupil ipads** with filtered access to the internet via BYOND. These are for use solely on the school site. Filtered access is allowed to the internet. App installation and changing of settings only by approved members of staff. Technical support is provided by Warwickshire LA. Use of images in accordance with School guidance on the taking and storage of images. No access to cloud services.
- **Staff ipads** with filtered access to the internet via BYOND. These are for use in school and out of school. Personal use is allowed. Filtered access is allowed to the school provided internet. App installation as required. Ipads are school property and are cleared of personal data/programs when returned as the staff member is leaving. The Use of images is in accordance with School guidance on the taking and storage of images. Technical support is provided by Warwickshire LA. Access allowed to cloud services.
- **Staff laptops** with full access to the network and filtered access to the internet via BYOND. These are for use in school and out of school. Personal use is allowed. Laptops are school property and are cleared of personal data/programs when the staff member leaves the school. Technical support is provided by Warwickshire LA. Use of images in accordance with School guidance on the taking and storage of images.

- **School owned mobile phones** without access to the internet. These are for use offsite. Personal use is not allowed. Use of images in accordance with School guidance on the taking and storage of images

Personal devices:

- Only staff and school owned ipads are given access to BYOND.
- School ipads will be stored in the secure charging trolley in the ICT store. Charged at night and used in accordance with the Ipad and laptop risk assessment.
- Other mobile devices are not to be used for school business

7.0 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 cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- **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 students / pupils are published on the school website / social media / local press**
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *pupils* in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, 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 students / 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.

- Pupil’s work can only be published with the permission of the pupil and parents or carers.

8.0 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”.
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs) (Head teacher/ Assistant Head)
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner’s Office.

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.
- Personal data should not be stored on any portable computer system, memory stick or any other removable media:

9.0 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:

Communication Technologies	Staff and other Adults				Pupils			
	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 the 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 / cameras				X				X
Use of other mobile devices e.g. tablets, gaming devices		X					X	
Use of personal email addresses 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

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 should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).

- **Users must immediately report, to the head teacher – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**
- **Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, 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 social media must not be used for these communications.
- Pupils at KS2 will be provided with individual school email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

10.0 Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools 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 or local authority group liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimize 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

School staff should ensure that:

- No reference should be made in social media to 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 *school* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school 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 school 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 school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to 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 school
- The school should effectively respond to social media comments made by others according to a defined policy or process

11.0 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. 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 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 out of school only	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make,	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					X

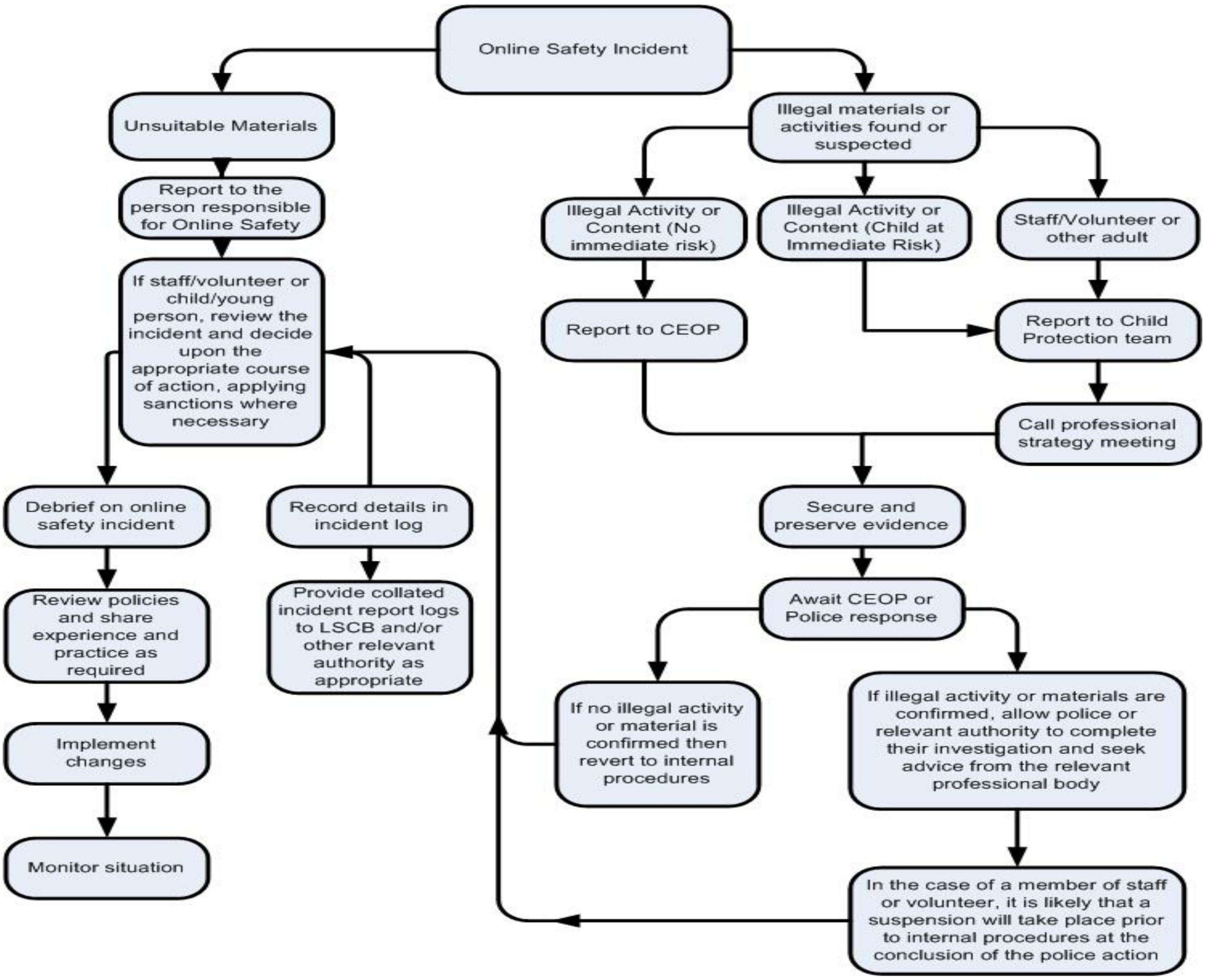
	against children Contrary to the Sexual Offences Act 2003.					
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (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					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			

12.0 Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

12.1 Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

12.2 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 / 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 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.

12.3 School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students / Pupils Incidents	Refer to class teacher / tutor	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	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 (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
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X						x	X
Unauthorised / inappropriate use of social media / messaging apps / personal email	X						x	x
Unauthorised downloading or uploading of files	X	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	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 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	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 's filtering system		x			x	x	x	X

Accidentally accessing offensive or pornographic material and failing to report the incident		X			x	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			x	x	x	X

Staff Incidents	Refer to Local Authority /	Refer to Police	Refer to Technical Support Staff for action re filtering	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				
Inappropriate personal use of the internet / social media / personal email				X		
Unauthorised downloading or uploading of files				X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account				X		
Careless use of personal data e.g. holding or transferring data in an insecure manner				X		
Deliberate actions to breach data protection or network security rules					X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software					X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature					X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X					
Actions which could compromise the staff member's professional standing						X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school					X	X

Using proxy sites or other means to subvert the school’s ’s filtering system				X		X
Accidentally accessing offensive or pornographic material and failing to report the incident				X		
Deliberately accessing or trying to access offensive or pornographic material				X	X	X
Breaching copyright or licensing regulations				X		X
Continued infringements of the above, following previous warnings or sanctions					X	

Appendices

Appendix 1: Pupil acceptable use agreement

Appendix 2: Parent/ Carer acceptable use agreement

Appendix 3: Use of Digital / Video images

Appendix 4: Staff and volunteer acceptable use policy agreement

Appendix 5: School Technical Security Policy (including filtering and passwords)

Appendix 1: Pupil Acceptable Use Agreements

Acceptable Use Policy Agreement (Years 3 & 4)

To keep me safe when I use a computer/iPad:

- I understand that the school will monitor my use of the internet, computers and iPads.
- I will keep my username and password to myself.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will keep personal information to myself.
- I will immediately tell an adult if I see something which upsets me on the screen.

When using a computer/iPad:

- I will respect others' work and will not change another user's files.
- I will be polite and responsible when I communicate with others and I will respect other people's opinions. This includes when I use my school email account and use the VLE.
- I will only use my USB if I have permission from my teacher.
- I will immediately report any damage or faults to my teacher, however this may have happened.
- I will only open hyperlinks in emails or attachments if I trust or know the person who sent the email.
- I will not install or attempt to install programmes of any type on any school device, nor will I try to alter computer settings.

I understand that the school will take action if I am unkind to members of the school community on online devices. In addition, if I fail to follow these rules, I may lose access to the school network/internet/computer/iPad and my parents/guardians may be informed.

I ………………………………………… (pupil) agree to follow these guidelines when I use the school systems and devices (in and out of school). This includes when I communicate using the school email and VLE.

Class:

Signed:

Date:

Acceptable Use Policy Agreement (Years 5 & 6)

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 username and password safe and secure – I will not share it, 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 be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line **(this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)**
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line. **Discuss who they could report to.**

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

- I understand that the *school* systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- 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 use the *school* systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

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 otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute **(give out)** images of anyone without their permission.
- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in the *school* , I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
  When in school:
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software to my teacher, however this may have happened.

- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, 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 not install or attempt to install programmes of any type on any school device, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:

- I should 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 try to download copies **(including music and videos)**
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

- I understand that the *school* also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I may lose access to the school network / internet. I understand that the school may contact my parents/guardians and in the event of illegal activities involve the police.

I ……………………………………….(pupil) agree to follow these guidelines when I use the school systems and devices (in and out of school). This includes when I communicate using the school email and VLE.

Group / Class: ....

Signed: ....

Date: ....

.

Appendix 2: Parent / Carer Acceptable Use Agreement

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

This Acceptable Use Policy is intended to ensure:

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

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

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

Parent / Carer Permission Form

Parent / Carers Name: ....

Pupil Name:..

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

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

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

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

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

Signed: ....Date: ....

Appendix 3: Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Students / Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students / pupils* in the digital / video images.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree

Digital / Video Images Permission Form

Parent / Carers Name: ....

Student / Pupil Name: ....

As the parent / carer of the above student / pupil, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.	Yes / No
I agree that if I take digital or video images at, or of – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes / No

Signed: ....

Date: ....

Appendix 4: Staff (and Volunteer) Acceptable Use Policy Agreement

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

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school 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 *pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, Learning platform etc.) out of school, and to the transfer of personal data (digital or paper based) out of school .

I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using *school* ICT 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 (eg on the school website / Learning platform) 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. (See Social networking policy)
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist 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 Protected and restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

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

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

Staff / Volunteer Name: ....

Signed: ....

Date: ....

Appendix 5

School Technical Security Policy (including filtering and passwords)

Introduction

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

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

Responsibilities

The management of technical security will be the responsibility of the head teacher.

Technical Security

Policy statements

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 receive guidance and training and will be effective in carrying out their responsibilities.

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.

There will be regular reviews and audits of the safety and security of school technical systems

- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained WCC staff.
- **All users will have clearly defined access rights to school technical systems.** *Details of the access rights available to groups of users will be recorded by Technical Staff*

- Users will be made responsible for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. *(See Password section below).*
- WES ICT 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
- Mobile device security and management procedures are in place
- School 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.
- Remote management tools are used by WCC staff to control workstations and view users activity
- An appropriate system is in place (Contact the head teacher) for users to report any actual / potential technical incident to the Online Safety Coordinator / Network Manager / Technician (or other relevant person, as agreed).
- An agreed policy is in place (Requests submitted to Admin office) for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school system.
- An agreed policy is in place (Section 11 Online Safety policy) regarding the extent of personal use that users (staff / pupils) and their family members are allowed on school devices that may be used out of school.
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices.
- All school networks and systems will be protected by secure passwords that are regularly changed
- The “master / administrator” passwords for the school systems, used by the technical staff are also be available to the Headteacher and kept in the school safe.
- All users (adults and young people) will have responsibility for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords for new users and replacement passwords for existing users will be allocated by School admin.
- Where passwords are set / changed manually requests for password changes should be authenticated by (the Admin office) to ensure that the new password can only be passed to the genuine user.

Staff Passwords

- All staff users will be provided with a username and password by admin office who will keep an up to date record of users and their usernames.
- the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters
- must not include proper names or any other personal information about the user that might be known by others
- the account should be "locked out" following six successive incorrect log-on attempts
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school

Pupil Passwords

- All users will be provided with a username and password by admin office who will keep an up to date record of users and their usernames.
- Pupils will be taught the importance of password security
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children. (Letters and numbers)

Training / Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's online safety policy and password security policy
- through the Acceptable Use Agreement

Pupils will be made aware of the school's password policy:

- in lessons (taught Computing lessons)
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The responsible person (head teacher) will ensure that full records are kept of:

- *Security incidents related to this policy*

Filtering

Introduction

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

Responsibilities

The responsibility for the management of the school's filtering policy will be held by WCC. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, No changes will be made to the school filtering service.

All users have a responsibility to report immediately to the ICT/ Computing coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists . Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The school has provided differentiated user-level filtering through the use of the Smooth wall web filtering system. (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils)
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher.
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems
- Any filtering issues should be reported immediately to the filtering provider.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the online safety education programme.in Computing lessons. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions at new to year group meetings/ newsletter etc.

Changes to the Filtering System

Changes to the filtering system will not be made.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement. *Monitoring will take place as follows: Policy Central software as utilised by WCC will be used, with monthly reports to the headteacher on users use of key words.*