ONLINE SAFETY POLICY

Written by Mrs L Barnes

Dec 2016

Contents

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by the Online Safety Committee

- Headteacher – Mrs Pattison
- Online Safety Subject Leader– Mrs Barnes
- Staff – including Teachers, Support Staff, Technical staff
- Governors
- Parents and Carers
- Community users
- Pupil Computing Committee

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

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body on:	*Dec 2016*
The implementation of this Online Safety policy will be monitored by the:	*Online Safety Committee*
Monitoring will take place at regular intervals:	*Each Autumn Term or when needed if prior to this*
The Governing Body Committee will discuss the implementation of the Online Safety Policy at regular intervals:	*At least once a year at Full Governors Meeting*
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:	*As and when required or at least each academic year.*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Officer,* *Police*

The school will monitor the impact of the policy using:

- Monitoring logs of internet activity (including sites visited) / filtering
- Logs of reported incidents
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - students / pupils
    - parents / carers
    - staff

Scope of the Policy

This policy applies to all members of Clitheroe St. James' school community who have access to and are users of our school ICT 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. In the case of both acts, action will only be taken over issues covered by the published 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 of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities 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 from Mr Mark Clayton, *Online Safety Governor*. The role of the Online Safety *Governor* will include:

- regular meetings with the Online Safety Subject Leader, Mrs L Barnes
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors

Headteacher

- The Headteacher has a duty of care for ensuring the safety (including online safety) the school community, though the day to day responsibility for online safety which will be delegated to the Online Safety Subject Leader.
- The Headteacher and a member of the Senior Leadership Team / are 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 is responsible for ensuring that the Online Safety Subject Leader 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 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.* (

Online Safety Subject Leader:

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

Network Manager / Technical staff:

The Network Manager / Technical Staff / Subject Leader for Computing is responsible for ensuring:

- that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack
- that the *school* meets required online safety technical requirements
- that the Online Safety Policy is followed.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- 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*

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)
- they report any suspected misuse or problem to the *Headteacher / Online Safety Coordinator / Officer* for investigation / action / sanction
- all digital communications with students / 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 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*

Designated Safeguarding Lead / Designated Person / Officer

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
- online-bullying

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. This group is also part of the safeguarding group. The group will be responsible for regular reporting to the *Governing Body*.

Members of the Online Safety Group (or other relevant group) will assist the Online Safety Coordinator (or other relevant person, as above) with:

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

Pupils:

- are responsible for using the *school* digital technology systems in accordance with the Pupil Acceptable Use Agreement
- 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 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. The *school* will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website, Facebook, Learning Platform and information about national / local online safety campaigns / literature.* Parents and carers will be encouraged to support the *school / academy* in promoting good online safety practice and to follow guidelines on the appropriate use of:

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

Community Users

Community Users who access school systems / website / Learning Platform as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school / academy systems.

Education – Students / Pupils

Whilst regulation and technical solutions are very important, their use will be balanced by educating *students* to take a responsible approach. The education of *pupils* in online safety is therefore an essential part of our school's online safety provision. Children will learn to recognise and avoid online safety risks and build their resilience. Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways:

- A planned online safety curriculum is provided as part of Computing / PHSE / other lessons and is regularly revisited.
- Key online safety messages are reinforced as part of a planned programme of assemblies.
- Pupils are 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 are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are supported in building resilience to radicalisation by providing a safe environment for debating issues and are helped to understand how they can influence and participate in decision-making.
- *Pupils understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school*
- *Staff act as good role models in their use of digital technologies the internet and mobile devices*
  in lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and 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 will be vigilant in monitoring the content of the websites the children visit.*
- *It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Computing Subject Leader can temporarily remove those sites from the filtered list for the period of study.*

Education – Parents / Carers or The Wider Community

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, web site, Learning Platform*
- *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*
- *Providing family learning courses in use of new digital technologies, digital literacy and online safety*
- *The school / academy website will provide online safety information*

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 annually or as required.

- 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. Online Safety BOOST includes unlimited online webinar training for all staff (https://boost.swgfl.org.uk/)
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school / academy Online Safety Policy and Acceptable Use Agreements.
- *It is expected that some staff will identify online safety as a training need within the performance management process and courses can be attended.*
- *The Online Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.*
- *This Online Safety Policy and its updates will be presented to and discussed by staff in staff / INSET days.*
- *The Online Safety Coordinator will provide advice / guidance / training to individuals as required.*

Training – Governors / Directors

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

- Attendance at training session
- Participation in school information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

The school along with the IT technician is responsible for ensuring that the schools network is as safe and secure as is reasonably possible that policies and procedures approved within this policy are implemented. It is also essential that the whole school will be effective in carrying out their online safety responsibilities:

- School technical systems are managed in ways that ensure that the school meets recommended technical requirements
- There are regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling will be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users are provided with a username and password. Users are responsible for the security of their username and password.
- The Computing Subject leader 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 is filtered by Lightspeed. 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 ensures that children are safe from terrorist and extremist material when accessing the internet.
- *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.*
- 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" (e.g. trainee teachers, supply teachers, visitors) onto the school systems. Downloading content and use of removable media is monitored.
- *Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.*

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices which are school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilizing 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 is consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behavior Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety education programme.

- The school Acceptable Use Agreements for staff, pupils/students and parents/careers 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[1]	Student owned	Staff owned	Visitor owned
Allowed in school	*Yes*	*Yes*	*Yes*	*No*[2]	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*No*

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

[2] The school should add below any specific requirements about the use of mobile / personal devices in school

Aspects that the school consider for *School owned / provided devices:*

- *Who they will be allocated to*
- *Where, when and how their use is allowed – times / places / in school / out of school*
- *If personal use is allowed*
- *Levels of access to networks / internet (as above)*
- *Management of devices / installation of apps / changing of settings / monitoring*
- *Network / broadband capacity*
- *Technical support*
- *Filtering of devices*
- *Access to cloud services*
- *Data Protection*
- *Taking / storage / use of images*
- *Exit processes – what happens to devices / software / apps / stored data if user leaves the school*
- *Liability for damage*
- *Staff training*

Personal devices:

- Which users are allowed to use personal mobile devices in school (staff / pupils / students / visitors)
- Restrictions on where, when and how they may be used in school
- Storage
- Whether staff will be allowed to use personal devices for school business
- Levels of access to networks / internet (as above)
- Network / broadband capacity
- Technical support (this may be a clear statement that no technical support is available)
- Filtering of the internet connection to these devices
- Data Protection
- The right to take, examine and search user's devices in the case of misuse (England only) – nab this must also be included in the Behaviour Policy.
- Taking / storage / use of images
- Liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility).
- Identification / labelling of personal devices
- How visitors will be informed about school requirements
- How education about the safe and responsible use of mobile devices is included in the school Online Safety education programmes.

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 students / 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 will inform and educate pupils about the risks associated with the taking, using, sharing, publishing and distribution of images. In particular, they will learn to 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 where other parental consent has not been sought.
- 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. Only children whose parental permission has been given, can be used.
- 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 teachers' 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

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 will 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)
- Risk assessments are carried out
- 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 is a policy for reporting, logging, managing and recovering from information risk incidents
- 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.

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

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

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 the school / academy	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 / academy 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.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and 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 / academy systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Whole class / group email addresses may be used at KS1, while pupils at KS2 and above may be provided with individual school email addresses for educational use.*
- *Pupils will be taught about online safety issues, such as the risks attached to the sharing of personal details. They will 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.*

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 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;
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents / careers 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 minimize 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 behavior 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

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:

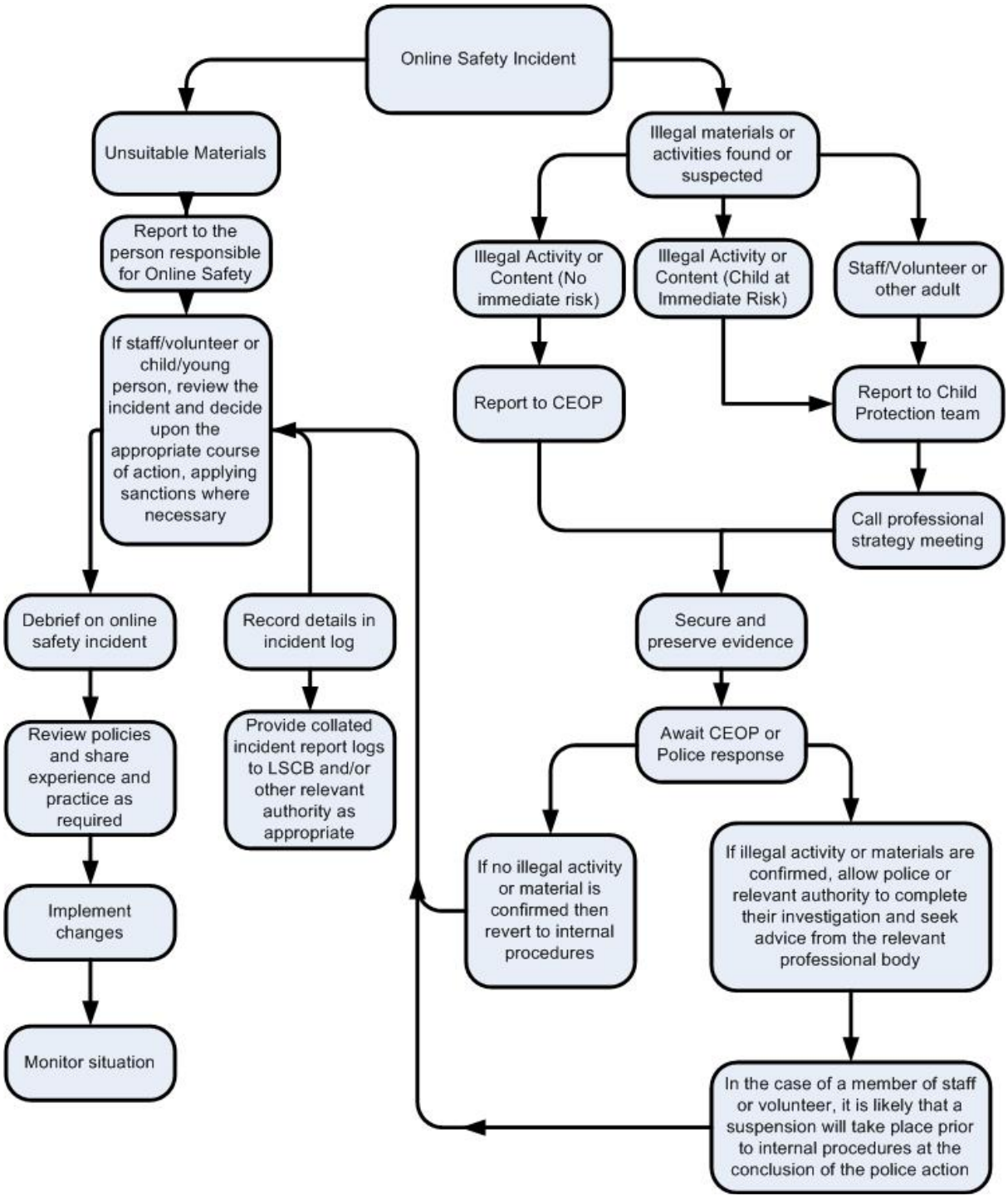
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. 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		

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).

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.



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 children 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.
    - 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.

School / Academy 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: (

	Actions / Sanctions								
Students / Pupils Incidents	Refer to class teacher	Refer to Deputy Head	Refer to Headteacher	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 e.g. 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	X	X
Unauthorised use of non-educational sites during lessons	X		X			X		X	
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X		X			X		X	
Unauthorised / inappropriate use of social media / messaging apps / personal email	X		X			X			X
Unauthorised downloading or uploading of files	X		X			X		X	
Allowing others to access school / academy network by sharing username and passwords	X		X			X		X	
Attempting to access or accessing the school / academy network, using another 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		X	

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X		X	X	X	X	
Continued infringements of the above, following previous warnings or sanctions	X	X	X		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	X	X	X
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X	X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material			X	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X		X	X	X	X	X

Actions / Sanctions

Staff Incidents

	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X			X	X
Inappropriate personal use of the internet / social media / personal email		X	X	X			X	X
Unauthorised downloading or uploading of files		X				X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X			X	X		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			X		X

Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		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
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X	X	X		X		X
Actions which could compromise the staff member's professional standing		X	X			X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school / academy		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	X		X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X	X	X	X
Breaching copyright or licensing regulations		X	X			X		X
Continued infringements of the above, following previous warnings or sanctions		X	X	X	X	X		X

Appendix

Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from: http://swgfl.org.uk/products-services/esafety/resources/creating-an-esafety-policy

Appendices

Pupil Acceptable Use Policy Agreement – FS/Key Stage 1

This Acceptable Use Policy

We endeavor to teach our children to be responsible users of ICT and provide them with the guidance necessary to keep them safe when using online technologies. The school will try to ensure that our children will have good access to ICT to enhance their learning, but in return will expect the children to agree to be responsible users.

This is how we stay safe at Key Stage 1 when we use computers:

- I will ask *a teacher / an adult* if I want to use the computer.
- I will only use activities that *the teacher /an adult* has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from *the teacher / an adult* if I am not sure what to do or if I think I have done something wrong.
- I will tell *the teacher / an adult* if I see something that upsets me on the screen.
- I know not to chat to anyone online.
- I will keep my personal information and passwords safe.
- I will always be nice if I do post or put up messages online.
- I know that if I break the rules I might not be allowed to use the computer.

All pupils need to sign in the box below to show that they have heard, read, understood and agree to the Pupil Acceptable Use Agreement.

Pupil Name:	Class:	**I understand the Pupil Acceptable Use Agreement.**

Pupil Acceptable Use Policy Agreement – Key Stage 2

This Acceptable Use Policy

We endeavor to teach our children to be responsible users of ICT and provide them with the guidance necessary to keep them safe when using online technologies. The school will try to ensure that our children will have good access to ICT to enhance their learning, but in return will expect the children to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use the school's ICT resources in a responsible manner, to make sure that I keep myself and others safe whilst working online.

Personal Safety

- I will keep my passwords safe and will not use other people's passwords
- I will be aware of "stranger danger", when working online.
- I will not share personal information about myself or others when on-line.
- I will not upload any images of myself or of others without permission
- I will not arrange to meet up with people that I have communicated with online.
- I will immediately report any inappropriate material; messages I receive or anything that makes me feel uncomfortable when I see it online.
- I will learn how to use the '***thinkuknow***' web site to keep myself safe.
- I will report any bad behavior by telling a responsible adult and will learn about using the CEOP Report button.
- I know that the school can look at my use of ICT and see the footprint of what I use online

ICT Property and Equipment

- I will respect all computer equipment and will report any damage or faults.
- I will respect others' work and will not access, copy, move or remove files.
- I will not use mobile phones/USB devices in school.
- I will not use any programs or software without permission.
- I will not use or open email, unless I know and trust the person or organization.
- I will not install programs or alter any computer settings.

Cyber Bullying

- I will be polite when I communicate with others
- I know not to do online what I wouldn't do offline (like in the playground)
- I will not use inappropriate language or make unkind comments
- I appreciate others may have different opinions

- I will not upload or spread images of anyone

The Internet

- I understand that I need permission to be on the Internet.
- I will not fill in any online forms without adult permission
- I will not use any sites I've not had permission to use, this includes social media sites that I'm not old enough to use
- I will learn about copyright laws and make sure I acknowledge resources
- I will not upload or download images, music or videos without permission
- I will check that the information that I access on the internet is accurate, as I understand that the internet may not be truthful and may mislead me.

Mobile Phones

- I know that mobile phones are not allowed to be used during the school day and are advised to be left at home, if brought to school it must be switched off and kept at the office.
- I know not to use text, voice messages, take images or use any internet connection to bully, upset or shock anyone in and out of school.
- I know that no images or videos should be taken on any mobile phones or personally-owned mobile devices without the consent of the person or people it involves.
- I know that the school is not responsible for any loss or damage to my mobile phone or any device I bring onto the school site.
- I understand that the school have a right to confiscate, search and keep any evidence on any mobile devices I bring into school.
- I know that I should protect my phone number by only giving them to trusted friends and family.

Outside of the School Community

- I understand that this agreement is for in and outside the school
- I know there will be consequences if I am involved in incidents of inappropriate behavior covered in this agreement which maybe a police matter.

All pupils need to sign in the box below to show that they have read, understood and agree to the Pupil Acceptable Use Agreement.

I understand the Pupil Acceptable Use Agreement for using technology, internet, email and online tools safely.

Pupil Name:	Class:

Parent/Carer E-Safeguarding and Acceptable Use Policies Information

As part of the programme of activities in school, all pupils have the opportunity to access a wide range of communication technology resources. These resources are an essential part of promoting children's learning and development; however, we also recognize the potential risks associated with these technologies. We therefore have an E-Safeguarding and Acceptable Use Policies in place in school.

In recent years, social networking sites such as Facebook and Twitter have grown in popularity and many people use them to communicate with family and friends, as we do to our school family. The vast majority of people who use social networking show respect in their communication with others and is something we must encourage to show our children that we are positive 'digital role models'. However, there are times when people disregard the rules and will use social networking sites to cyberbully and harass others.

Recently, there have been a number of high-profile cases in the media where people have used the internet to intimidate and bully others. The police have investigated these cases and in some instances have led to criminal prosecutions.

As a school, we encourage our parents to support us with the education and wellbeing of their children and if at any time, parents feel they have issues regarding their child's education or with school matters, they should see their class teacher. If the issue has not been resolved, then an appointment can be made with the Head Teacher. We also have a complaints policy on the school website if deemed necessary.

If an incident is reported to school staff, it should be investigated and, if school deem it appropriate, will be acted upon by the school's Head teacher. In extreme cases, the Head teacher would consider whether it appropriate to notify the police or solicitors to take further action.

Therefore, as a Parent/Carer, you are asked to:

- Read the **Parent/Carers Acceptable Use Agreement**
- Read and talk to your child about their **Pupil Acceptable Use Agreement**
- Parent/Carer and child to sign their agreements.
- Return one signed copy of the agreement to School and keep a copy to refer to.

If you disagree with any of the rules within the agreements or feel there is an area of Internet Safety you feel is not being developed, please contact the Head teacher.

Please remember, all children in school are taught how to keep safe and be responsible when they are online, whether they are at school or at home. As children are able to access the internet outside school, whether this is at home, a friend's house or on a mobile device, we need to work in partnership with you the parent/carer to keep our children safe.

Parent / Carer and Pupil Acceptable Use Agreement Form

Parent / Carer Acceptable Use Agreement:

- I have read and discussed the agreement with my child and confirm that he/she has understood what the rules mean.
- I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials through a managed filtered system.
- I understand that occasionally, inappropriate materials may be accessed and accept that the school will endeavor to deal with any incident that may arise, according to policy.
- I agree that the school is not liable for any damages arising from use of the Internet facilities.
- I understand that my son's/daughter's activity will be monitored and that the school will contact me if they have concerns about any possible breaches of the Internet Safety Rules or Pupil Acceptable Use Agreement.
- I understand not to upload any photos of St James' pupils at any school event (for example, assemblies'/sports days/plays or school trips) onto a social media site.
- I understand that everything posted on a social networking site should be deemed as open to the public and it is therefore unacceptable to use this as a forum for posting inappropriate or malicious comments about the school or any members of the school community.

All parents need to sign in the box below to show that they have read, understood and agree to the Acceptable Use Agreement.

Parent/Carer Signature:	Date:

Please return the slip below to the office to say that both yourself and your child has read, understood and agreed to the Acceptable Use Agreement.

Pupil Name:	Class:

Pupil Signature:	Date:

Parents/Guardians Name:	Signature

PERMISSION FOR THE USE OF PHOTOGRAPHS & DIGITAL IMAGES

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your child. We follow these rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video. **Please tick accordingly & return to school by Fri 16th September -**

I give my permission for photographs and digital media of my child to be used in school displays, in St James' printed publications, on the schools' online profiles, for example: the school website, Facebook page and in videos on YouTube or, with school permission, other types of media associated with the school i.e. press releases, St. James' Church.

By giving permission I also understand that this means once any images/videos are on the school profiles/website, they are also in the public domain on the World Wide Web. ☐

I do not give my permission for photographs and digital media of my child to be used in school displays, in St James' printed publications, on the schools' online profiles, for example: the school website, Facebook page and in videos on YouTube or, with school permission, other types of media associated with the school i.e. press releases, St. James' Church. ☐

When attending school functions and taking photographs of your child please take appropriate images that do not contain other people's children (unless consent is given by their parents) and only upload images of your child when distributing on social media sites.

PERMISSION FOR THE USE OF THE INTERNET.

I give my permission for my child to use the Internet as part of their everyday learning whilst at school according to the AUP (see attached). ☐

I do not give my permission for my child to use the Internet as part of their everyday learning whilst at school.

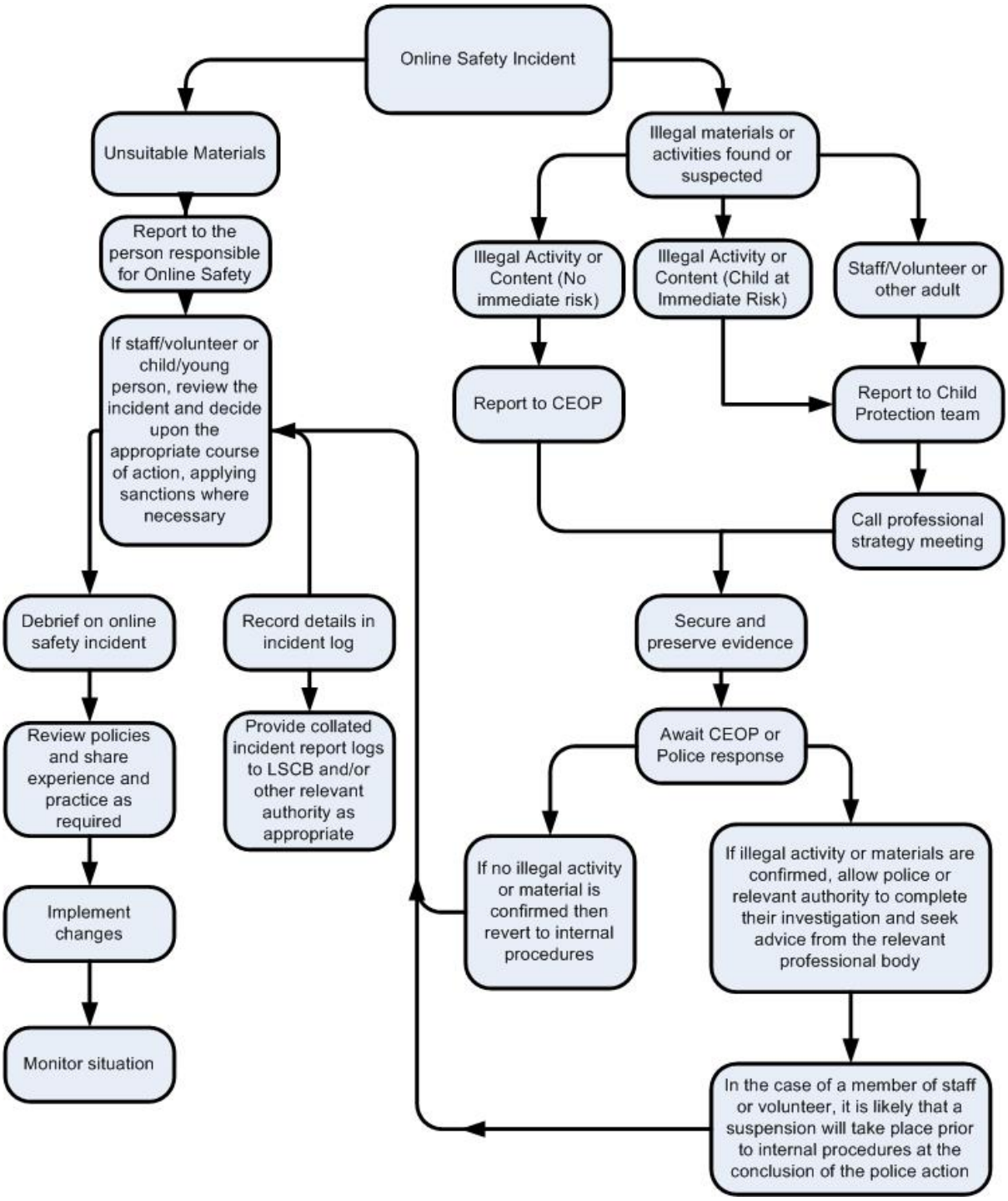
☐ **If I wish at any time to withdraw my child from the above, I will inform the office in writing.**

This permission will last for the whole of your child's education at this school.

Child:_____ Class: _____

Signed:_____ Date: _____

Responding to incidents of misuse – flow chart



Record of reviewing devices / internet sites (responding to incidents of misuse)

Group: .....

Date: .....

Reason for investigation: .....

.....

.....

.....

Details of first reviewing person

Name: .....

Position: .....

Signature: .....

Details of second reviewing person

Name: .....

Position: .....

Signature: .....

Name and location of computer used for review (for web sites)

.....

.....

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken

Reporting Log

Group: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Training Needs Audit Log

Group: .....

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date

Legislation

Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is an anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers to search for electronic devices. It also provides powers to search for data on those devices and to delete data.)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Glossary of Terms

AUP / AUA	Acceptable Use Policy / Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)

SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.