STONEBRIDGE SCHOOL

E-SAFETY POLICY

FEBRUARY 2018

POLICY STATEMENT

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 E-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 can 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 / carers of incidents of inappropriate E-safety behaviours that take place out of school.

It is the responsibility of the school to ensure that the Network Manager and all technical staff carry out all the E-safety measures that would otherwise be the direct responsibility of the school. It is important that the Network Manager is fully aware of the *school* E-safety Policy and Acceptable Use Policy. The school will also check their Local Authority and other relevant body policies on these technical issues.

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

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

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

With an increase in use of all types of social media for professional and personal purposes this policy sets out clear guidance for staff to manage risk and behaviour online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. Ofsted's E-safety inspection framework reviews how a school should protect and educate staff and pupils in their use of technology, including the measures that would be expected to be in place to intervene and support should a particular issue arise. Schools are increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.

ROLES AND RESPONSIBILITIES

The following section outlines the E-safety roles and responsibilities of individuals and groups within the *school.*

GOVERNING BOARD:

Governors are responsible for the approval of the E-safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about E-safety incidents and monitoring reports. The member of the *Governing Board* who has taken on the role of *E-safety Governor* is the Chair of Governors who is also the Safeguarding Governor. The role of the E-safety *Governor* will include:

- regular meetings with the E-safety Co-ordinator
- regular monitoring of online incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meeting

HEAD TEACHER

- The *Headteacher* has a duty of care for ensuring the safety (including E-safety) of members of the school community, the day to day responsibility for E-safety will be delegated to the *E-safety Co-ordinator who will be a Deputy Designated Safeguarding Lead.*
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious E-safety allegation being made against a member of staff. (see flow chart on dealing with E-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant *Local Authority HR / other relevant body* disciplinary procedures). https://boost.swgfl.org.uk/
- *The Headteacher is responsible for ensuring that the E-safety Coordinator and other relevant staff receive suitable training to enable them to carry out their E-safety roles and to train other colleagues, as relevant.* https://boost.swgfl.org.uk/
- *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 E-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.*
- *The Senior Leadership Team will receive regular monitoring reports from the E-safety Co-ordinator.*

E-SAFETY CO-ORDINATOR

The E-Safety Co-ordinator at Stonebridge School is the Deputy Designated Safeguarding Lead. They are responsible for:

- taking day to day responsibility for E-safety issues and having a leading role in establishing and reviewing the school E-safety policies and documents.
- ensuring that all staff are aware of the procedures that need to be followed in the event of an E-safety incident taking place.
- providing training and advice for staff
- liaising with the Local Authority and relevant bodies
- liaising with school technical staff
- receiving reports of E-safety incidents and creating a log of incidents to inform future E-safety developments, https://boost.swgfl.org.uk/

- meeting regularly with the E-safety *Governor and Designated Safeguarding Lead* to discuss current issues and to review incident logs and filtering control logs
- attending relevant Governors meetings.
- reporting regularly to Senior Leadership Team

NETWORK MANAGER AND TECHNICAL STAFF (INCLUDING COMPUTING CURRICULUM LEADER)

The Network Manager and Technical Staff are 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 E-safety technical requirements and any *Local Authority* E-safety Policy or guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with E-safety technical information in order to effectively carry out their E-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 and E-safety Coordinator* for investigation and appropriate action.
- *that monitoring software / systems are implemented and updated as agreed in school policies*

TEACHING & SUPPORT STAFF

Are responsible for ensuring that:

- they have an up to date awareness of E-safety matters and of the current *school* E-safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the *Headteacher / E-safety Coordinator* for investigation an appropriate action
- all digital communications with pupils and parents / carers should be on a professional level *and only carried out using official school systems*
- E-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the E-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
- *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 AND MEMBERS OF THE SAFEGUARDING TEAM

Should be trained in E-safety issues and be aware of the potential for serious child protection and 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

E-SAFETY GROUP

The E-Safety Group provides a consultative group that has wide representation from the *school*, with responsibility for issues regarding E-safety and the monitoring the E-safety Policy including the impact of initiatives. At Stonebridge School the E-Safety Group will comprise of The E- Safety Co-ordinator (Deputy DSL), The Headteacher (DSL), Members of the Technical team, The Inclusion Manager, the PSHE Curriculum Leader, members of the pupil wellbeing committee.

Members of the E-Safety Group will assist the E-Safety Coordinator with:

- the production, review and monitoring of the school E-Safety Policy.
- the review and monitoring of the school filtering system
- mapping and reviewing the E-safety curricular provision – ensuring relevance, breadth and progression
- monitoring incident logs
- consulting stakeholders – including parents / carers and pupils about the E-safety provision
- monitoring improvement actions identified through these meetings and through such audits (such as 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 (PAUP)
- having a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- needing to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- knowing and understand policies on the use of mobile devices and digital cameras
- knowing and understanding policies on the taking and use of images
- knowing about and understanding cyber-bullying.
- understanding the importance of adopting good E-safety practice when using digital technologies out of school and realising that the *school's* E-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 and information about national / local E-safety campaigns / literature.* Parents and carers will be encouraged to support the *school* in promoting good E-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
- their children's personal devices in the school (where this is allowed)
- their children's access to the internet

COMMUNITY USERS

Community Users who access school technology as part of the wider *school* provision will be expected to sign a Community User AUP before being provided with access to school systems.

PROCEDURES AND PRINCIPLES IN RELATION TO EDUCATION & TRAINING

EDUCATION - PUPILS

E-safety should be a focus in all areas of the curriculum and staff should reinforce E-safety messages across the curriculum. The E-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned E-safety curriculum will be provided as part of Computing, PHSE, Safeguarding and other lessons and will be regularly revisited
- Key E-safety messages will be reinforced as part of our programme of assemblies, pastoral activities, the curriculum and associated workshops
- Pupils will be taught in all lessons to be critically aware of the materials and the content they access on-line and be guided to validate the accuracy of information.
- Pupils will 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. (links to additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- Pupils will 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 will act as good role models in their use of digital technologies the internet and mobile devices
- pupils will be guided to sites checked as suitable for their use in lessons and processes will be in place for dealing with any unsuitable material that is found in internet searches.
- Pupils will be allowed to freely search the internet, staff will be vigilant in monitoring the content of the websites the young people visit.

EDUCATION – PARENT / CARERS

Many parents and carers have only a limited understanding of E-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and 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 / academy will therefore seek to provide information and awareness to parents and carers through:

- *Curriculum activities*
- *Letters, newsletters, web site*
- *Parents / Carers workshops and coffee mornings*
- *High profile events or campaigns e.g. Safer Internet Day*
- *Educational courses offered to increase technology skills*
- *Reference to the relevant web sites and publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers*

EDUCATION & TRAINING – STAFF & VOLUNTEERS

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

- A planned programme of formal E-Safety training will be made available to staff through the school based CPD programme & annual Safeguarding Training
- An audit of the E-safety training needs of all staff will be carried out regularly.
- Specific E-Safety training for members of the E-Safety Group
- All new staff receiving E-safety training as part of the induction programme, ensuring that they fully understand the school E-safety Policy and Acceptable Use Agreements.
- Identifying E-Safety as a training need within the performance management process.
- The E-Safety Coordinator and DSL receiving regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- The E-Safety Policy and its updates being presented to and discussed by staff in team meetings and school based CPD
- The E-Safety Coordinator and DSL providing advice, guidance and training to individuals as required.

TRAINING – GOVERNING BOARD

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

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

TECHNICAL – INFRASTRUCTURE, EQUIPMENT FILTERING & MONITORING

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their E-safety 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

• All users will have clearly defined access rights to school technical systems and devices.

• All users (including pupils) will be provided with a username and password by the School Technicians who will keep an up to date record of users and their usernames. Staff users are responsible for the security of their username and password and will be required to change their password when required by the internal system of the school.

• The "administrator" passwords for the school ICT system, used by the Network Manager and school based ICT technician must also be available to the Headteacher and kept in a secure place

• ICT Technicians are 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 LGFL and access is regularly monitored through the monitoring system in place.

• Internet filtering will ensure that children are safe from terrorist and extremist material when accessing the internet. (Nb. additional duties for schools academies under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.)

• The school has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different groups of users – staff and pupils)

• School technical staff will 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 or potential technical incident or security breach to the relevant person.

• Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

• An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.

• An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.

• An agreed policy is in place that outlines staff expectations for downloading executable files and installing programmes on school devices. (APU)

• A defence system is in place which protects the schools network / devices and is regularly updated. This protects the system from any possible threat from external removable media (eg memory sticks / CDs / DVDs) by users on school devices.

- The school's system can be accessed safely and securely via the VPN in place.

MOBILE TECHNOLOGIES

In considering the use of mobile technologies the school should consider possible issues and risks which may include: security risks in allowing connections to the school network, filtering of personal devices, breakages and insurance, access to devices for all students, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership. 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	✓	✓	✓		✓	✓
Full network access	✓	✓	✓			
Internet only					✓	✓
No network access				✓		✓

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.

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

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or 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. To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites. Parents / carers should not comment on any activities involving other pupils in any digital or video images.

[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.

• 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. 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 any 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 should only be published with the permission of the pupil and parents or carers.

COMMUNICATIONS

This is an area of rapidly developing technologies and uses. The following table shows how the school currently expects these technologies to be used in the school setting:

Staff & other adults	Student / 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	✓						✓	
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Take photos on mobile phones				✓				✓
Take photos on cameras	✓						✓	
Use of other mobile devices e.g. tablets, gaming devices	✓						✓	
Use of personal email addresses in school or on school network	✓							✓
Use of school email for personal emails	✓				✓			
Use of messaging apps				✓				✓
Use of social media				✓				✓
Use of blogs				✓				✓

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff 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 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 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, personal mobile numbers or social media must not be used for these communications.
- Pupils across the school will be provided with individual school email addresses for educational use.
- Pupils should be taught about E-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.

SOCIAL MEDIA – PROTECTING PROFESSIONAL IDENTITY

All schools 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 minimise risk of harm to pupils, staff and the school through:

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

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
- Understand that a breach of any expectations set out in this policy could result in disciplinary action being taken against them.

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 account. 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, those that do will be considered under the disciplinary procedures of the school.
- Where any personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

- The school network filtering does not allow access to social media sites.

Monitoring of Public Social Media

- As part of active social media engagement, the school will proactively monitor the Internet for public postings about the school key members of staff, this is considered good practice.
- The school should effectively respond to social media comments made by others according to a defined policy or process

The *school's* use of social media for professional purposes will be checked regularly by the E- Safety Group to ensure compliance with the school policies. E-safety BOOST Reputation Alerts that highlight any reference to the school in online media (newspaper or social media for example) will be put in place. https://boost.swgfl.org.uk/)

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 will also 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 Action	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal

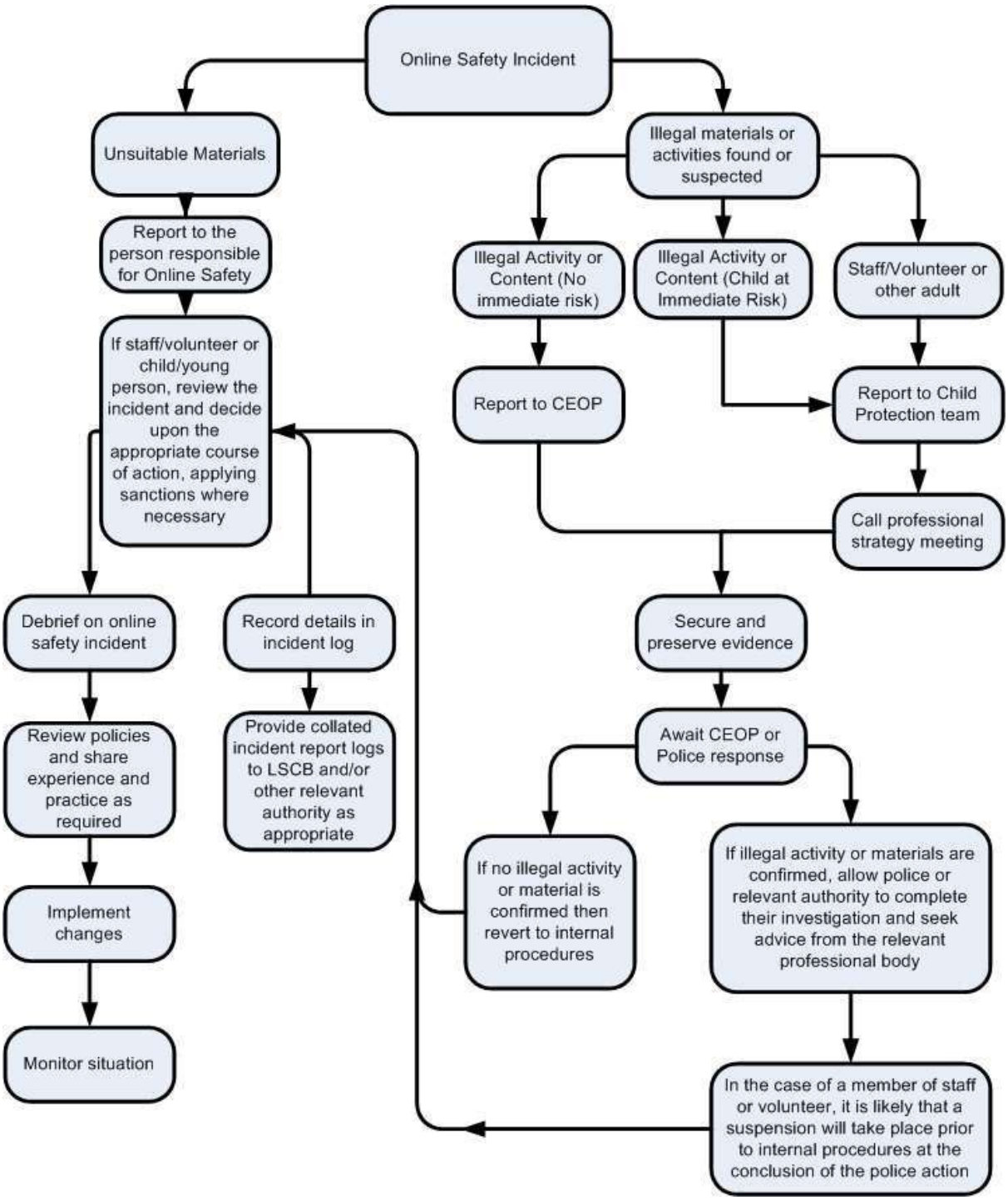
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments	Child sexual abuse images – The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					✓
	Grooming, incitement, arrangement or facilitation of sexual acts 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					✓
	Criminal racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) Contrary to The Public Order Act 1986					✓
	Pornography				✓	
	Promotion of any kind of discrimination				✓	✓
	Threatening behaviour, including promotion of physical violence or mental harm				✓	✓
	Promotion of extremism or terrorism				✓	✓
	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				✓	
Using school systems to run a private business					✓	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					✓	
Infringing copyright					✓	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
Unfair usage (downloading / uploading large files that hinders others in the use of the internet)					✓	
Online gaming (educational)					✓	
Online gaming (non- educational)					✓	
Online gambling					✓	
Online shopping				✓		
File sharing				✓		
Use of School based social media				✓		
Use of messaging apps				✓		
Use of video broadcasting e.g. YouTube		✓				

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.

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 the school will refer to the right hand side of the Flowchart (below and appendix) for responding to E-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 / 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.

- 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 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 o criminally racist material o promotion of terrorism or extremism
- Other criminal conduct, activity or materials

The computer in question should be isolated as is reasonably possible, 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 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:

Student / Pupil Incidents

	Refer to class teacher	Refer to head of year	Refer to Headteacher	Refer to the Police	Refer to technical support for action	Inform parent / carers	Removal of access rights to network / internet	Warning	Further action e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓					
Unauthorised use of non-educational sites during lessons						✓	✓	✓	✓
Unauthorised / inappropriate use of mobile phones / digital cameras / other mobile devices						✓		✓	
Unauthorised / inappropriate use of social media / messaging apps / personal email						✓		✓	✓
Unauthorised downloading or uploading of files								✓	
Allowing others to access school network by sharing usernames and passwords								✓	
Attempting to access the school network using another students / pupils account							✓	✓	
Attempting to access the school network using the account of a member of staff						✓	✓	✓	
Corrupting or destroying the data of others						✓	✓	✓	✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓		✓	✓	✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions				✓					
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school						✓	✓	✓	✓
Using proxy sites or other means to subvert the schools filtering system	✓	✓	✓		✓	✓	✓	✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident						✓		✓	
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓		✓	✓	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act					✓	✓		✓	✓

Actions / Sanctions

Staff Incidents

	Refer to line manager	Refer to Headteacher	Refer to Local Authority	Refer to the Police	Refer to technical support for action	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓	✓	✓	✓		
Inappropriate use of the internet / social media / messaging apps / personal email	✓	✓			✓	✓	✓	✓
Unauthorised downloading or uploading of files					✓	✓		
Allowing others to access school network by sharing usernames and passwords or attempting to access the school network using another person's account		✓			✓	✓		
Careless use of personal data e.g. holding or transferring data in an insecure manner		✓			✓	✓		
Deliberate actions to breach data protection or network security rules		✓			✓	✓		✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓			✓	✓		✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	✓	✓			✓	✓	✓	✓
Using personal email / social networking / instant messaging / text messaging to carry out digital communication with student's / pupil's		✓		✓				
Actions that would compromise the staff members professional standing	✓	✓			✓	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓				✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident			✓	✓	✓			
Deliberately accessing or trying to access offensive or pornographic material				✓				✓
Breaching copyright or licensing regulations							✓	
Continued infringements of the above, following previous warnings or sanctions								✓

SCHEDULE FOR DEVELOPMENT, MONITORING & REVIEW	
This E-Safety policy was approved by the Governors Curriculum & Standards Committee on:	*February 2018*
This E-Safety policy was approved by Staff on:	*February 2018*

The implementation of this E-safety policy will be monitored by the:	*E-Safety Group*
Monitoring will take place at regular intervals:	*At least once a year and additionally when the E-Safety group meets*
The Governing Board of the school will receive a report on the implementation of the E-safety Policy generated by the monitoring group (which will include anonymous details of any E-safety incidents) at regular intervals:	*At least once a year* *Heads Safeguarding Report (each half term)*
The E-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 E-safety or incidents that have taken place. The next anticipated review date will be:	*Spring Term 2019*
Should serious E-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* • *Internal monitoring data for network activity* • *Surveys / questionnaires of pupils, parents / carers and staff*