ST. AUGUSTINE OF CANTERBURY CATHOLIC PRIMARY SCHOOL

E-Safety Policy

Mission Statement

"I called you by your name, you are mine." Isaiah 43
The mission of our school is to support and further the teachings of Christ and His Church.
We welcome and embrace individuals of all abilities and cultural backgrounds.
We aim to enhance and celebrate their moral, physical, social and emotional development, so that they may reach their full potential in an atmosphere of stability, care and respect.
We believe that education is for all and in partnership with parents, carers, children and the wider Catholic community: we will strive and succeed in a wholly inclusive setting.

Date issued: February 2018

Date to be reviewed: February 2019

Written by: Mrs Claire Burns (Deputy DSL/E-safety lead)

In consultation with: Miss Lisa Richardson (Computing lead)

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by Mrs Claire Burns (Deputy Designated Safeguarding Lead, e-safety lead) in consultation with Miss Lisa Richardson (Computing lead), SLT, BCTEC (technicians), and all teaching staff.

It has been agreed by the Governing body, school council and all members of staff.

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Curriculum Committee on behalf of Governing Body on:

_____

The implementation of this e-safety policy will be monitored by the: E-Safety lead, computing Lead and the Senior Leadership Team.
Monitoring will take place annually and will be a component of Computing, PSHE and Anti-bullying monitoring.
The Governing Body will receive a report including anonymous details of e-safety incidents annually.
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: February 2019
Should serious e-safety incidents take place, the following external persons/agencies should be informed: LA ICT Manager Marc Dermody, Local Authority Designated Officer(s) (LADO team) by Telephone: 01634 331 065 Email: child.protection@medway.gov.uk.cjsm.net and the Police.

The school will monitor the impact of the policy using:

- Logs of reported incidents (using reporting template in appendix)
- Monitoring logs of internet activity (including sites visited) by the computing lead and BCTEC
- Internal monitoring data for network activity by the computing lead and BCTEC
- Surveys / questionnaires of
  - students / pupils
  - parents / carers
  - staff

Scope of the Policy

This policy applies to all members of the school community (including staff, children, volunteers, parents / carers, visitors, students/work experience) 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 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. 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 (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the school's Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

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

Governors:

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 annual information about e-safety incidents. A member of the Governing Body has taken on the role of E-Safety Governor – Karen McIntyre. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Lead
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors / committees under Safeguarding as an agenda item

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Lead.
- The Headteacher and Deputy Headteacher are 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 / LADO, see also Whistle-Blowing and Chid Protection policies).
- The Headteacher and Senior Leaders are responsible for ensuring that the E-Safety Lead and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is carried out by the Computing Lead – Miss Lisa Richardson supported by BCTEC and LA provider.
- The Senior Leadership Team will be updated by the E-Safety Lead of any reported incidents.

E-Safety Lead:

The E-safety lead - Mrs Claire Burns has the day to day responsibility for E-safety. These responsibilities include:

- day to day responsibility for E-safety issues and a leading role in establishing and reviewing the school E-safety policies / 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
- Monitoring the delivery of E-safety curriculum alongside the Computing lead – lesson observations/pupil conferencing
- liaising with the Local Authority / relevant body
- liaising with school Computing lead and school technical staff

- receiving reports of E-safety incidents and creates a log of incidents to inform future e-safety developments, see appendix for template.
- meeting with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- reporting to Senior Leadership Team

Network Manager / Technical staff:

At St. Augustine of Canterbury we have a managed ICT service provided by BCTEC. The school ensures that the managed service provider carries out all the E-safety measures.
BCTEC 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 E-safety technical requirements and Local Authority Guidance
- that users may only access the networks and devices through a properly enforced password protection
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with 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 / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and E-Safety Lead for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

All 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 Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher and E-Safety Coordinator 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
- E-safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the E-safety and acceptable use policies
- students / 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 and implement current policies with regard to these devices (see also use of digital and video images policy)
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead and Deputy DSL

DSL and Deputy DSL are trained in E-safety issues and are aware of the potential for serious safeguarding issues (including radicalisation) 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

Students / pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- 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 – using the CEOP reporting button
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good E-safety practice when using digital technologies out of school and realise 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 / VLE 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 and VLE
- their children's personal devices in the school

Teaching and learning

The Internet is a part of everyday life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. The vast majority of pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Internet access is an entitlement for pupils who show a responsible and mature approach to its use.

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- access to online educational resources;
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with Medway and DfE;
- Access to learning wherever and whenever convenient.

Education – students / pupils

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

Our rules for Staying Safe Online are:

1) Don't post any personal information online – like your address, email address or mobile number.
2) Think carefully before posting pictures or videos of yourself. Once you've put a picture of yourself online most people can see it and may be able to download it, it's not just yours anymore.
3) Keep your privacy settings as high as possible
4) Never give out your passwords
5) Don't befriend people you don't know
6) Don't meet up with people you've met online. Speak to your parent or carer about people suggesting you do
7) Remember that not everyone online is who they say they are
8) Think carefully about what you say before you post something online
9) Respect other people's views, even if you don't agree with someone else's views doesn't mean you need to be rude
10) If you see something online that makes you feel uncomfortable, unsafe or worried: leave the website, turn off your computer if you want to and tell a trusted adult immediately

http://www.safetynetkids.org.uk/personal-safety/staying-safe-online/ (See also the pupil acceptable use agreement)

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 delivered through the Rising Stars Computing scheme of work as well as regular focussed E-safety lessons, linked with our PSHE education provision.
- Key E-safety messages are reinforced as during assemblies linked to national E-safety awareness such as Safer Internet day
- Pupils are taught in all lessons where applicable, 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 helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

SEN

Children with Special Educational Needs (SEN) are included within all areas of the curriculum, including the use of the internet for educational, creative, empowering and fun ways, just like their peers. However, they may be particularly vulnerable to E-safety risks. For example:

- Children and young people with Autistic Spectrum Disorder may make literal interpretations of content, which will affect how they respond.

- Some children may not understand much of the terminology due to language delays or disorders.

- Some children with complex needs do not understand the concept of friendship, and therefore trust everyone implicitly. They do not know how to make judgements about what is safe information to share. This leads to confusion about why you should not trust others on the internet.

- There is also growing concern around cyberbullying. We need to remember that some children with SEN or disabilities may be vulnerable to being bullied through the internet, or not recognise that they are being bullied.

- In addition, some children may not appreciate how their own online behaviour may be seen by someone else as bullying.

These are challenging and complex issues which are addressed as part of any classroom differentiation or within individual children's learning plans, written in co-ordination with the Special Education Needs Co-ordinator (SENCO) Mrs Liggins, where relevant. Additional support for children with SEN can be found on Child's Net: http://www.childnet.com/resources/know-it-all-for-teachers-sen

E-safety brigade

The children in Year 6 form the members of the E-Safety brigade. They work together with the class teachers to promote E-safety in the other year groups. Together with the class teachers, the children plan lessons for the younger year groups to help them understand the importance of being safe on the internet.

Partnership with Medway Health Team

At St. Augustine of Canterbury we have strong links with the Medway Health team. The team provide our children with E-safety assemblies and have introduced us to an E-safety poster competition. The Medway health team have also facilitated parent sessions and staff training focussing on E-safety; as well as wider child protection issues, which often have an element of being Internet safe.

Education – parents / 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 / 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, VLE
- Parents / Carers evenings / sessions at least annually
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. CEOP https://www.thinkuknow.co.uk/parents/ 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:

- Staff will receive E-safety training through staff meetings, CPD and INSET.
- All new staff receive E-safety information as part of their induction programme, ensuring that they fully understand the school E-safety policy and Acceptable Use Agreements.
- The E-Safety Lead and/or Computing Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The E-Safety Lead and/or Computing Lead will provide advice / guidance / training to individuals as required.

Training – Governors

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

- Attendance at training provided by the Local Authority / National Governors
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons) where applicable.

Technical – infrastructure / equipment, filtering and monitoring

At St. Augustine of Canterbury we have a managed ICT service provided by BCTEC. The school ensures that the managed service provider carries out E-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements as required by the Local Authority
- 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 pupils will be use class log-ons and passwords
- The administrator passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher and Computing Lead and kept in a secure place
- The Computing Lead along with BCTEC 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 by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- The school has provided enhanced / differentiated user-level filtering for members of staff.
- BCTEC staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach using the BCTEC helpdesk.
- 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.
- Supply staff and visitors have temporary access onto the school systems through a separate log-on.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about

potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with the use of digital and video images policy.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website

Data Protection

The current Data Protection Act (DPA) will be replaced by the new and updated General Data Protection Regulation (GDPR) on 25th May 2018. At St. Augustine of Canterbury we are preparing for this new data protection regulation which is designed to strengthen and unify the safety and security of all data held within an organisation. This will comply with the 6 principles outlined in article 5, stating that:

The GDPR requires that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes or statistical

purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained and lawfully processed.
- It has clear and understood arrangements for the security, storage and transfer of personal data

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 (see also the Confidentiality policy/agreement).
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

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

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 during school hours	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x						x	
Use of mobile phones in lessons				x				x
Use of mobile phones in social time	x							x
Taking photos on mobile phones / cameras				x				x
Use of other mobile devices e.g. personal tablets, gaming devices				x				x
Use of personal email addresses in school, or on school network				x				x
Use of school email for personal emails				x				x
Use of social media (see also Confidentiality policy)				x				x

See also Mobile Phone Policy

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

- The official school email service (Medway mail) may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report - to Headteacher or E-safety Lead, 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, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

- Whole class email addresses may be used at KS1, while students / pupils at KS2 and above 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, 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 (see also the Confidentiality policy/agreement).

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 limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

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.

Unsuitable / inappropriate activities

St. Augustine of Canterbury believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

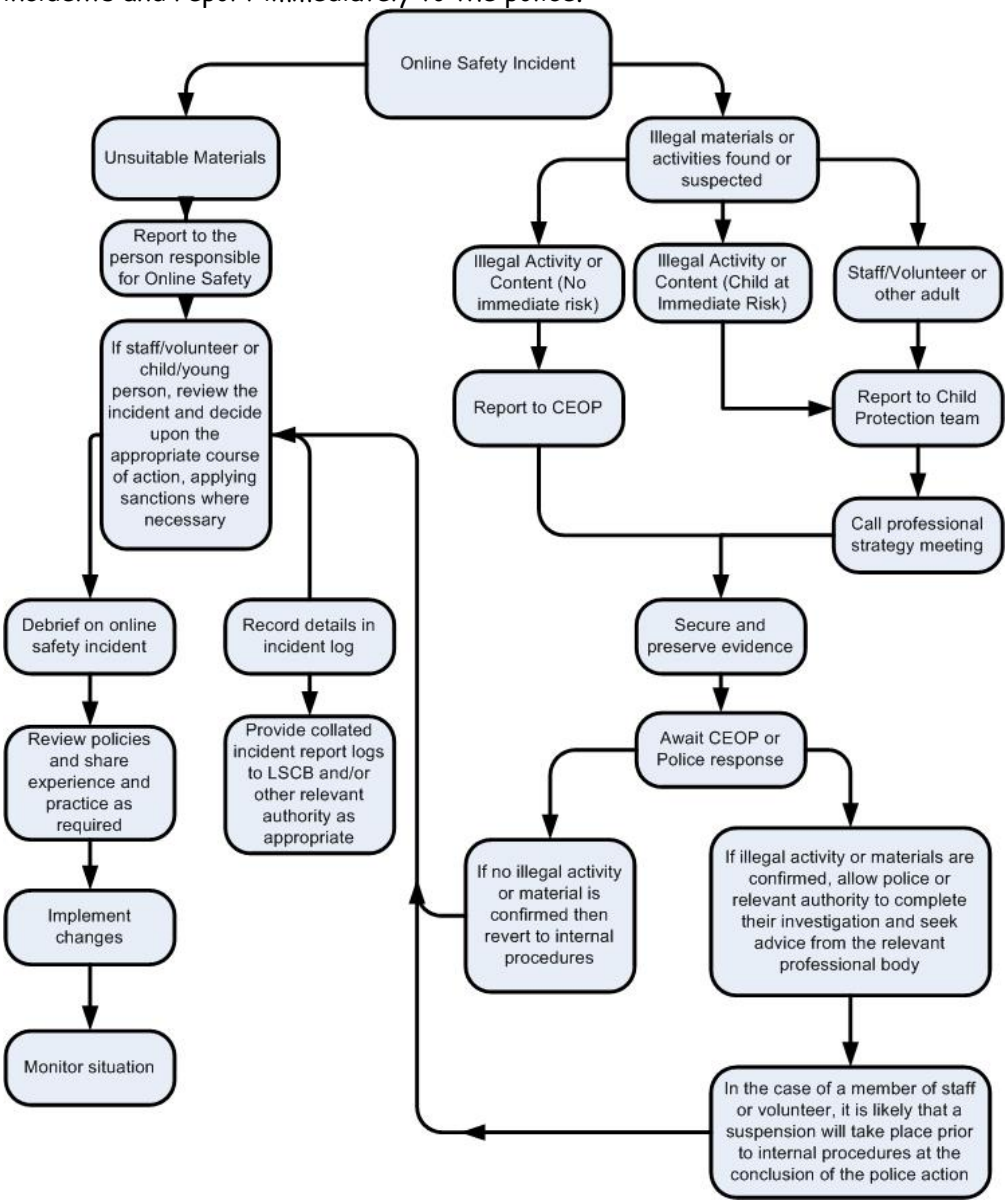
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / 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			
Use of social media					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) 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/governor involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - 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 child protection 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:

Students / Pupils Actions / Sanctions

Incidents:	Refer to class teacher	Refer to KS lead/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					
Unauthorised use of non-educational sites during lessons	X							X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X				X			
Unauthorised use of social media / messaging apps / personal email	X	X				X		X	
Unauthorised downloading or uploading of files	X	X						X	
Allowing others to access school network by sharing username and passwords	X							X	
Attempting to access or accessing the school network, using another pupil's account	X	X						X	
Attempting to access or accessing the school network, using the account of a member of staff		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	
Continued infringements of the above, following previous warnings or sanctions			X			X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X			X			
Using proxy sites or other means to subvert the school's / academy's filtering system			X		X				
Accidentally accessing offensive or pornographic material and failing to report the incident			X		X			X	
Deliberately accessing or trying to access offensive or pornographic material			X	X					X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X		X				

Staff Actions / Sanctions

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				
Inappropriate personal use of the internet / social media / personal email	X					X		
Unauthorised downloading or uploading of files		X			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		
Careless use of personal data e.g. holding or transferring data in an insecure manner		X			X	X		
Deliberate actions to breach data protection or network security rules		X	X			X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X			X		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X					X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X				X		
Actions which could compromise the staff member's professional standing		X	X			X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X				X		
Using proxy sites or other means to subvert the school's / academy's filtering system		X			X			
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X			X		
Deliberately accessing or trying to access offensive or pornographic material		X	X	X				X
Breaching copyright or licensing regulations		X	X		X			
Continued infringements of the above, following previous warnings or sanctions		X	X					X

Appendix

Reporting Log Template

Reporting Log Group										
Date	Time	Incident	Incident Reported by	Signature	Action taken					
					What?	By whom?				

NSPCC

Sample e-safety incident report form

Name of school:		
Your details		
Your name:	Your position:	Date and time of incident:
Details of e-safety incident		
Date and time of incident:		
Where did the incident occur? i.e. at school or at home:		
Who was involved in the incident? Child/young person ☐ Name of child..... Staff member/ volunteer ☐ Name of staff member/ volunteer..... Other ☐ please specify.....		
Description of incident (including IP addresses, relevant user names, devices and programmes used)		
Action taken: ☐ Incident reported to head teacher/senior manager ☐ Advice sought from Safeguarding and Social Care ☐ Referral made to Safeguarding and Social Care ☐ Incident reported to police ☐ Incident reported to Internet Watch Foundation ☐ Incident reported to IT ☐ Disciplinary action to be taken ☐ E-safety policy to be reviewed/amended ☐ Other (please specify)		
Outcome of investigation:		

Acknowledgements

http://www.swgfl.org.uk/Staying-Safe/Creating-an-E-Safety-policy

https://www.nspcc.org.uk/globalassets/documents/information-service/esat-briefing-sample-e-safety-incident-report-form.pdf

https://www.thinkuknow.co.uk/parents/ http://www.childnet.com/parents-and-carers

http://www.safetynetkids.org.uk/personal-safety/staying-safe-online/

Further Information and Support

Please see Internet Matters for definitions of different technologies:
https://www.internetmatters.org/advice/glossary/

The following is not exhaustive but should provide a useful starting point (KCSIE 2016):

www.thinkuknow.co.uk
www.disrespectnobody.co.uk
www.saferinternet.org.uk
www.internetmatters.org
www.childnet.com/cyberbullying-guidance
www.pshe-association.org.uk
https://educateagainsthate.com
www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

www.gov.uk/UKCCIS - external visitors and online safety (KCSIE 2018 – draft)