RIVERSDALE PRIMARY SCHOOL

Online Safety Policy

Date:
Review Date:
Signed: _____ (Governor)
Signed: _____ (Headteacher)

INTRODUCTION

Riversdale Primary School takes the safety of all children and adults very seriously. This policy is written to protect all children and adults. We recognise that Online Safety, also referred to as eSafety, encompasses not only internet technologies, but also electronic communications such as mobile phones and wireless technology.

Other Linked Policies:

1. Virtual Learning Environment Policy
2. Social Media Policy
3. Acceptable Use Policy
4. Photographic and Video Images Policy
5. Data Protection Policy & Data Disposal Appendix

What does electronic communication include?

- Internet collaboration tools: social networking sites and web-logs (blogs);
- Internet research: websites, search engines and web browsers;
- Mobile phones
- Internet communications: email and IM;
- Webcams and videoconferencing;
- Wireless games consoles.

Internet technologies and electronic communications provide children and young people with opportunities to broaden their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with the way these technologies can be used.

This Online Safety Policy should recognise and seek to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for others.

These risks are caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to Students and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to considered illegal activity.

This policy, as well as associated policies, including the Data Protection Policy, School Facebook Page Policy and Photographic and Video Images Policy, have been updated and modified to comply with the requirements of the General Data Protection Regulation, also referred to as GDPR, 2018.

What are the risks?

- Receiving inappropriate content;
- Predation and grooming;
- Requests for personal information;
- Viewing 'incitement' sites;
- Bullying and threats;
- Identity theft Publishing inappropriate content;
- Online gambling;
- Misuse of computer systems;
- Publishing personal information;
- Hacking and security breaches;
- Corruption or misuse of personal data.

A summary of a school's safety responsibilities is outlined below. This list will assist in developing a co-ordinated and effective approach to managing e-safety issues.

- The school will review the policy regularly and revise the policy annually to ensure that it is current and considers any emerging technologies.
- The school will audit their filtering systems regularly with LGFL to ensure that inappropriate websites are blocked.
- To ensure that Students and staff are adhering to the policy, any incidents of possible misuse will need to be investigated.
- The school will include e-Safety in the curriculum and ensure that every pupil has been educated about safe and responsible use. Students need to know how to control and minimise online risks and how to report a problem. We use the SAFE materials to carry this out.
- All staff must read and sign the Acceptable Use Policy.
- Parents should sign and return the Student Acceptable Use Policy.
- The Online Safety Policy will be made available to all staff, governors, parents and visitors through the website.

Implementation and Compliance

No policy can protect students without effective implementation. It is essential that staff remain vigilant in planning and supervising appropriate, educational ICT experiences.

INDIVIDUAL ROLES & 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/Sub Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of ICT Link Governor which includes Online Safety. The role will include:

- regular meetings with the Computing Lead
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors meetings

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Computing 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 online safety allegation being made against a member of staff (see flow chart on dealing with online safety incidents "Responding to incidents of misuse" and relevant Local Authority disciplinary procedures).
- The Headteacher/Senior Leaders are responsible for ensuring that the Computing Lead 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/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 online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Computing Lead.
- Ensure that all members of the school community comply with all aspects of the GDPR that relate to sharing personal data, with a lawful basis, through online means, including images of pupils, parents/carers and staff.

Online Safeguarding Lead:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensure that parents/carers are aware of the most up to date information regarding online safety by providing guides and leaflets through the school website, Weduc and school social media accounts
- 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 where necessary
- 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 the Computing Lead to discuss current issues and plan Online Safety lessons/events
- meets regularly with Computing Link Governor to discuss current issues, review incident logs and filtering/change control log
- attends relevant Governors meetings
- reports regularly to Senior Leadership Team
- ensure that all members of the school community comply with all aspects of the GDPR that relate to sharing personal data, with a lawful basis, through online means, including images of pupils, parents/carers and staff.

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/Safeguarding officers where appropriate
- all digital communications with students/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
- students understand and follow the Online Safety Policy and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students 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
- Ensure that they comply with all aspects of the GDPR that relate to sharing personal data, with a lawful basis, through online means, including images of pupils, parents/carers and staff.

Designated Safeguarding Lead & Deputy DSL:

Should be trained in Online Safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Students:

- are responsible for using the school digital technology systems in accordance with the 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 cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers:

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

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

TEACHING AND LEARNING:

Students:

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

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

- A planned online safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students should be helped to understand the need for the student 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 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 are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Parents/Carers:

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, website
- Parents/Carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant websites / publications

Staff:

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Computing Lead will receive regular updates through attendance at external training events.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/ INSET days.
- The Computing Lead will provide advice / guidance / training to individuals as required.

Governors:

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

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

GENERAL POLICY STATEMENTS:

Why is Internet use important?

Developing effective practice in Internet use for teaching and learning is essential. 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. The Internet use is part of the statutory curriculum and a necessary tool for learning. The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

Students use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security. The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of Students. Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of Students;
- Staff should guide Students in on-line activities that will support the learning outcomes planned for the Students' age and maturity;
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Evaluating Internet Content:

In a perfect world, inappropriate material would not be visible to Students using the Internet, but this is not easy to achieve and cannot be guaranteed. It is a sad fact that Students may occasionally be confronted with inappropriate material, despite all attempts at filtering. Students should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: to close the page and report the incident immediately to the teacher.

Safeguarding & Youth Produced Imagery

Why do we teach young people about youth produced sexual imagery?

Teaching about safeguarding issues in the classroom can prevent harm by providing young people with skills, attributes and knowledge to help them navigate risks. Addressing sensitive issues promotes a whole school approach to safeguarding; giving young people the space to explore key issues and the confidence to seek the support of adults should they encounter problems.

Keeping Children Safe in Education statutory guidance states that schools 'should ensure children are taught about safeguarding, including online, through teaching and learning opportunities'.
In line with this, schools should provide young people with opportunities to learn about the issue of youth produced sexual imagery.

How do we teach young people about youth produced sexual imagery?

Learning about youth produced sexual imagery cannot be taught in isolation. Learning should be located within a developmental PSHE education programme, as well as in the school's computing programme where it should reflect the requirements of the National Curriculum programme of study for computing. Teaching should also reflect the principles articulated in 'Key principles of effective prevention education' - produced by the PSHE Association on behalf of NCA-CEOP.

Given the potential sensitivity of these lessons it is essential that this issue is taught within an emotionally safe classroom climate where clear ground rules have been negotiated and established and where boundaries around teacher confidentiality have been clarified. If during any lesson teachers suspect any child or young person is vulnerable or at risk the school's safeguarding protocols should always be followed.

We consider:

- What specific learning is provided in the curriculum about youth produced sexual imagery? This focuses on factual information and will include:
    - what it is
    - how it is most likely to be encountered
    - the consequences of requesting, forwarding or providing such images, including when it is and is not abusive
    - issues of legality
    - the risk of damage to peoples' feelings and reputation
- What specific learning is provided to ensure children and young people have the strategies and skills required to manage:
    - specific requests or pressure to provide (or forward) such images
    - the receipt of such images

This will include who to tell; what to say; what to do; what not to do and where to get support from within and outside of the school.

It is important to recognise how difficult it may be for children and young people to challenge or deny their peers' requests for images, especially those to whom they are attracted or whose approval they seek. It may also be extremely difficult for them to ask adults for help. Young people may have made a decision they now regret and may find it difficult or embarrassing to ask for help. It is essential that lessons help children and young people develop the confidence they may need to put their skills and strategies into action.

It is therefore important that children and young people understand their school's policy towards youth produced sexual imagery. The content of this policy and the protocols the school will follow in the event of an incident can be explored as part of this learning. This reinforces the inappropriate nature of abusive behaviours and can reassure children and young people that their school will support them if they experience difficulties or have concerns.

When do we teach young people about these issues?

It is essential that learning is both age and readiness appropriate and is seen by children and young people as balanced and relevant to their real life experience. Therefore, as a school we introduce this concept slowly and when it is felt that a class is emotionally ready for this topic.

Local Area Network security

- Users must act reasonably;
- Users must take responsibility for their network use. For all staff, flouting electronic use policy is regarded as a matter for dismissal;
- Workstations should be secured against user mistakes and deliberate actions, e.g. deleting files and folders;
- Servers will be located securely and physical access restricted;
- The server operating system will be secured and kept up to date;
- Virus protection for the whole network will be installed and current;
- Access by wireless devices must be pro-actively managed.

Wide Area Network (WAN) security

All Internet connections must be arranged via LGFL to ensure compliance with the security policy. Firewalls and switches are configured to prevent unauthorised access between schools.

- The security of the school information systems will be reviewed regularly;
- Virus protection will be updated regularly;
- Security strategies will be discussed with the LA when necessary;
- Personal data sent over the Internet should be encrypted or otherwise secured;
- Portable media may not be used without specific permission followed by a virus check;
- Unapproved system utilities and executable files will not be allowed in Students' work areas or attached to email;

- Files held on the school's network will be regularly checked;
- The ICT coordinator / network manager will review system capacity regularly.

Virtual Learning Environment (VLE)

- Please see the Virtual Learning Environment Policy for details regarding this.

Emails

- Although students have an @riversdaleschool.org.uk account, the email facility will be disabled;
- Students must be taught that, should they possess a personal email account, they must immediately tell a trusted adult (for example a teacher) if they receive offensive email;
- Students must be taught not to reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission;
- Contact can take place via the Google Classroom which can be monitored carefully by staff.

School Website

The contact details on the website should be the school address, e-mail and telephone number. Staff or Students' personal information must not be published. Email addresses should be published carefully, to avoid spam harvesting. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Use of Images

- Under the terms of the General Data Protection Regulations (GDPR) 2018, all photographs and video images of children and staff alike are classified as personal data. This means that an image can not be used for public display or for school publicity etc. unless there is a ***lawful basis*** for this and that the child as the owner of the personal data, or the parent/carer where the child is not of suitable maturity to make such decisions, has been made aware/given consent. The most applicable lawful basis in this instance is ***consent***.
- When using digital images, staff should inform and educate students 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 ***consent*** from parents or carers will be obtained before photographs of students are published on the school website/social media/local press via the ***Photographic and Video Image Consent Form*** signed at when the student is enrolled at the school.
- 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 is not covered by the General Data Protection Regulation 2018). To respect everyone's privacy and in some cases protection, these images must not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students 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, ensuring compliance with the GDPR 2018. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's work can only be published with the permission of the student / pupil and parents or carers.

Social Networking

- The school will block/filter access to social networking sites;
- Newsgroups will be blocked unless a specific use is approved;
- Children will be taught about the role of CEOP (Child Exploitation and Online Protection) and how to contact such organisations;
- Students will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc;
- Students should be advised not to place personal photos on any social network space;
- They should consider how public the information is and consider using private areas;
- Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school;
- Teachers should be advised not to run social network spaces for student use on a personal basis.

Filtering

The school will work with LGFL the Internet Service Provider to ensure that systems to protect Students are reviewed and improved. If staff or Students discover unsuitable sites, the URL must be reported to the Online Safety Lead. This task requires both educational and technical experience. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Video Conferencing

School video conferencing equipment should not be taken off school premises without permission because use over the non-educational network cannot be monitored or controlled. At present the school has access to Google Meets through the Google For Education package. Students will have access to this function in order to participate in live lessons that may take place during times of national lockdown. The school settings will ensure that students are not able to set up meetings and therefore will be unable to attend meetings without staff member presence to ensure high levels of safeguarding.

Users

Unique login and password details for the educational video conferencing services should only be issued to members of staff and kept secure. Students should ask permission from the supervising teacher before making or answering a video conference call. Video conferencing should be supervised appropriately for the Students' age. Parents and guardians should agree for their children to take part in videoconferences, probably in the annual return.

Mobile phones

- We understand that some children will bring in mobile phones, for example for parent reassurance if they are walking to and from school by themselves. However, they are required to hand in their phones to the teacher at the start of the day.
- Children must be reminded that they should immediately tell a trusted adult if they receive an offensive message either via email, text message or social media.

Personal Data

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations (2018):

- 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 high level protection such as encryption.

This school:

- Uses individual, audited log-ins for all staff users;
- Storage of all data within the school will conform to the UK data protection requirements and subsequent General Data Protection Regulation (GDPR).
- Students and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

Internet Access

- The school will maintain a current record of all staff and Students who are granted access to the school's electronic communications;
- All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource;
- At Key Stage 1 and 2, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials;
- Parents will be asked to sign and return a consent form for pupil access.

INTERNET RISKS

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Wandsworth Council can accept liability for the material accessed, or any consequences resulting from Internet use.

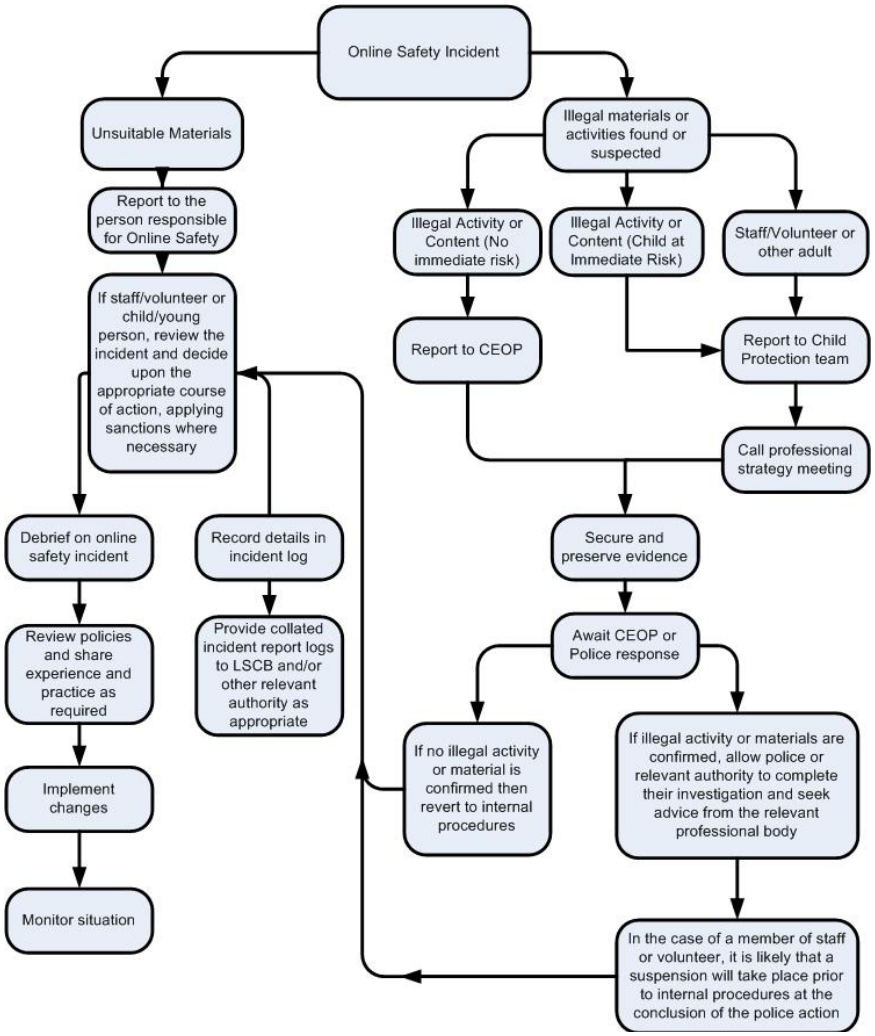
The school will audit ICT use to establish if the online safety policy is adequate and that the implementation of the policy is appropriate. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly.

Online Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff;
- All children will be taught to use the internet safely and the role of CEOP to monitor and report abuse;
- Any complaint about staff misuse must be referred to the Head Teacher, unless it is the Head Teacher where complaints will be sent to the Chair of Governors;
- Students and parents will be informed of the complaints procedure;
- Parents and Students will need to work in partnership with staff to resolve issues.

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 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 / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).

Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.
It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Introducing the Policy

- Safety rules will be posted in rooms with Internet access;
- Students will be informed that network and Internet use will be monitored;
- Safety training will be introduced to all to raise the awareness and importance of safe and responsible internet use;
- Instruction in responsible and safe use should precede Internet access;
- An e-safety module will be included in the PSHE, Citizenship or ICT programmes covering both school and home use;
- All staff will be given the School e-Safety Policy and its application and importance explained;
- Staff should be aware that Internet traffic can be monitored and traced to the individual user;
- Discretion and professional conduct is essential;
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues;
- Parents' attention will be drawn to the school's e-Safety Policy in newsletters, the school brochure and on the school learning platform;
- Internet issues will be handled sensitively, and parents will be advised accordingly.

This policy will be reviewed annually.

Appendix: Websites offering additional advice and guidance

BBC Chat Guide
http://www.bbc.co.uk/chatguide/

Becta
http://www.becta.org.uk/schools/Online Safety

Childline
http://www.childline.org.uk/

Child Exploitation & Online Protection Centre
http://www.ceop.gov.uk

Grid Club and the Cyber Cafe
http://www.gridclub.com

Internet Watch Foundation
http://www.iwf.org.uk/

Internet Safety Zone
http://www.internetsafetyzone.com/

Kidsmart
http://www.kidsmart.org.uk/

NCH – The Children's Charity
http://www.nch.org.uk/information/index.php?i=209

NSPCC
http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm

Schools e-Safety Blog
http://clusterweb.org.uk?Online Safetyblog

Schools ICT Security Policy
http://www.eiskent.co.uk

Stop Text Bully
www.stoptextbully.com

Think U Know website
http://www.thinkuknow.co.uk/

UK Council for Child Internet Safety (UKCCIS)
https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Virtual Global Taskforce – Report Abuse
http://www.virtualglobaltaskforce.com/