eSafety and Internet Usage Policy

(Including Acceptable Use Agreements)

2020-2023

Signed by Chair..... Date.....

E Safety And Internet Usage

E safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's E safety policy will operate in conjunction with other school policies including but not limited to: Behaviour, Anti-Bullying and Safeguarding.

Background - Why Is Internet Use Important?

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 information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the internet is therefore an entitlement for pupils who show a responsible and mature approach to its use and School has a duty to provide pupils with quality internet access.

Many pupils will access the internet outside school and will need to learn how to evaluate online information and to take care of their own safety and security.

How Does Internet Use Benefit Education?

Benefits of using the internet in education include:

- access to world-wide educational resources including museums, libraries and art galleries
- rapid and cost effective worldwide communication
- inclusion in the National Education Network which connects all UK schools
- educational and cultural exchanges between pupils worldwide
- 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 support services and professional associations
- improved access to technical support including remote management of
- access to learning wherever and whenever convenient

Good Habits

E safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of E-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the provider including the effective management of content filtering.
- National Education Network standards and specifications.

Dangers To Consider

Some of the dangers children may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information

- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyberbullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. We must demonstrate that we provide the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. The E safety policy that follows explains how we intend to do this.

Policy Outline

This policy applies to all members of the school (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 Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of 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 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 at regular intervals in line with key review dates. The Governing Body will:

- receive reports and meet with the E-Safety Coordinator as required
- monitor e-safety incident logs
- recommend changes to policy should an incident occur that requires it
- seek support of appropriate bodies where further guidance is required
- keep up to date with the school's systems
- report to relevant board/committee within the trust

Headteacher and Senior Leaders

The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community. They will ensure that the relevant protections are in place to safeguard others and minimise the risk of/for abuse of the internet or IT software/hardware.

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. They are also responsible for ensuring that the relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

Safeguarding Designated Person/Safe Team

The Safe Team should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

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

E-Safety Coordinator

The eSafety lead takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing e-safety policy and practice.

They will:

- keep up to date with e-safety technical information in order to effectively carry out their e-safety role
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff as appropriate
- liaises with the relevant body within the school, trust or LA
- liaises with technical staff and related bodies
- receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments
- meet with the head and/or Governors to discuss current issues, review incidents and filtering
- attend relevant meetings
- reports regularly to Senior Leadership Team

IT Coordinator

The ICT/Computing lead is responsible for ensuring that:

- the school's technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets required e-safety technical requirements stipulated by the DfE and the Trust

- users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the usage of the school internal and external network, internet and email is regularly monitored in order that any misuse can be reported

All of the above is done under the guidance or direction of XP Trust and technical support staff from ACS/Adept and Realsmart. The school recognises the increasing complexities of monitoring infrastructure integrity and does not expect staff to work in isolation on these matters.

School Staff

By accepting employment at the school, all staff agree to abide completely by the guidance outlined in this and all school policies. Failure to comply could result in disciplinary action and/or dismissal.

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 report any suspected misuse or problem to the Headteacher for investigation
- all digital communications with pupils or 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 and acceptable use policies
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- if any inappropriate material is loaded/discovered, the device in question is taken by the member of staff either to the lead or other appropriate body who will decide on what needs to happen
- the lesson is stopped and all use of devices until further notice if deemed appropriate to ensure safety is maintained

School Pupils

All pupils are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy. They must always follow the instructions of staff and should immediately and without hesitation cease the use of or hand over any technology if requested to do so. Failure to comply could result in sanctions and in extreme cases, exclusion.

They should all:

- have a good understanding of research skills and appropriate use of the internet
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- know and understand policies on the use of mobile devices and digital cameras. They should also know and understand the concept of cyber-bullying.

- 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 and Guardians

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and 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 or local e-safety campaigns and appropriate 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 or related social media accounts
- their children's personal devices in the school (where this is allowed)

It is also crucial that parents and guardians also follow safe practice as role models for their children. All parents and guardians should:

- protect their children from accessing or discovering age inappropriate content either online or otherwise
- carefully monitor screen time to ensure children are not vulnerable to exploitation from others or exposed to inappropriate language or content from a third party
- ensure games played on consoles are age appropriate

By accepting a place at the school, parents and guardians are by default agreeing to the following non-negotiable principles themselves:

- consider how they communicate using social media and other public platforms where their voice could be used inappropriately
- make sure they do not participate in any online defamation of character relating to the school, its staff and especially its pupils
- remove any content from their social media accounts immediately if the school deems it to be harmful or damaging to others or the reputation of the school

Failure to comply could result in the involvement of third parties such as social services, the police or legal action.

Safety Measures in School

To help keep your children and all users safe when using technology in school, we take the following steps:

- Internet provision from a reputable source
- Hardware based Firewalls to prevent intrusion
- Hardware and software based Internet Filtering Solution maintained by IT professionals
- Software firewalls to provide additional layers of security
- Enterprise class Antivirus Software managed by IT professionals
- Server class architecture and physical domains managed by IT professionals
- G-Suite user interface and cloud based architecture managed by IT professionals

- Data protected by Google Enterprise Class service
- Secure Enterprise level encryption for access including security certificates to be installed on devices to access the school wifi network
- Approved and blocked web content filters maintained by IT professionals

In addition to the above:

- All hardware devices are managed and monitored by IT professionals
- Any pupil mobile devices are only admitted into the building with prior permission
- Devices such as phones for safe travel to and from school are immediately handed in to the office on arrival and are only returned upon departure
- Software and apps used have all been vetted and pre-approved prior to install/usage
- Children are not permitted to use any device without the prior approval of a member of staff
- Devices are stored in secure areas monitored by staff
- Educate the children in how to stay safe online through:
    - our curriculum
    - assemblies
    - external visitors
    - bespoke support to individuals where needed

Capture of images/media and Publication to Websites including Social Media

In order to maintain a presence on the web to promote school events and share information with parents and guardians, school staff are required to take photographs of children. All school staff have undertaken a full police check and undertake regular disclosure reviews to protect the safety of the pupils. Any photographs taken will be solely for the use of promoting the school internally or externally.

By attending the school, you consent to the use of images to promote school events within approved school media such as the school website and school twitter accounts. This is done to share and celebrate the life and journey of your children and to promote the exciting events taking place within school.

To protect your child's integrity, the school will:

- Never link a child's full name and image in public media without express written consent for a specific purpose
- Only use christian names by default when describing/narrating content with images
- Always seek consent before allowing a third party such as Doncaster Free Press to use a child's image or name in their publications

Visitors to school

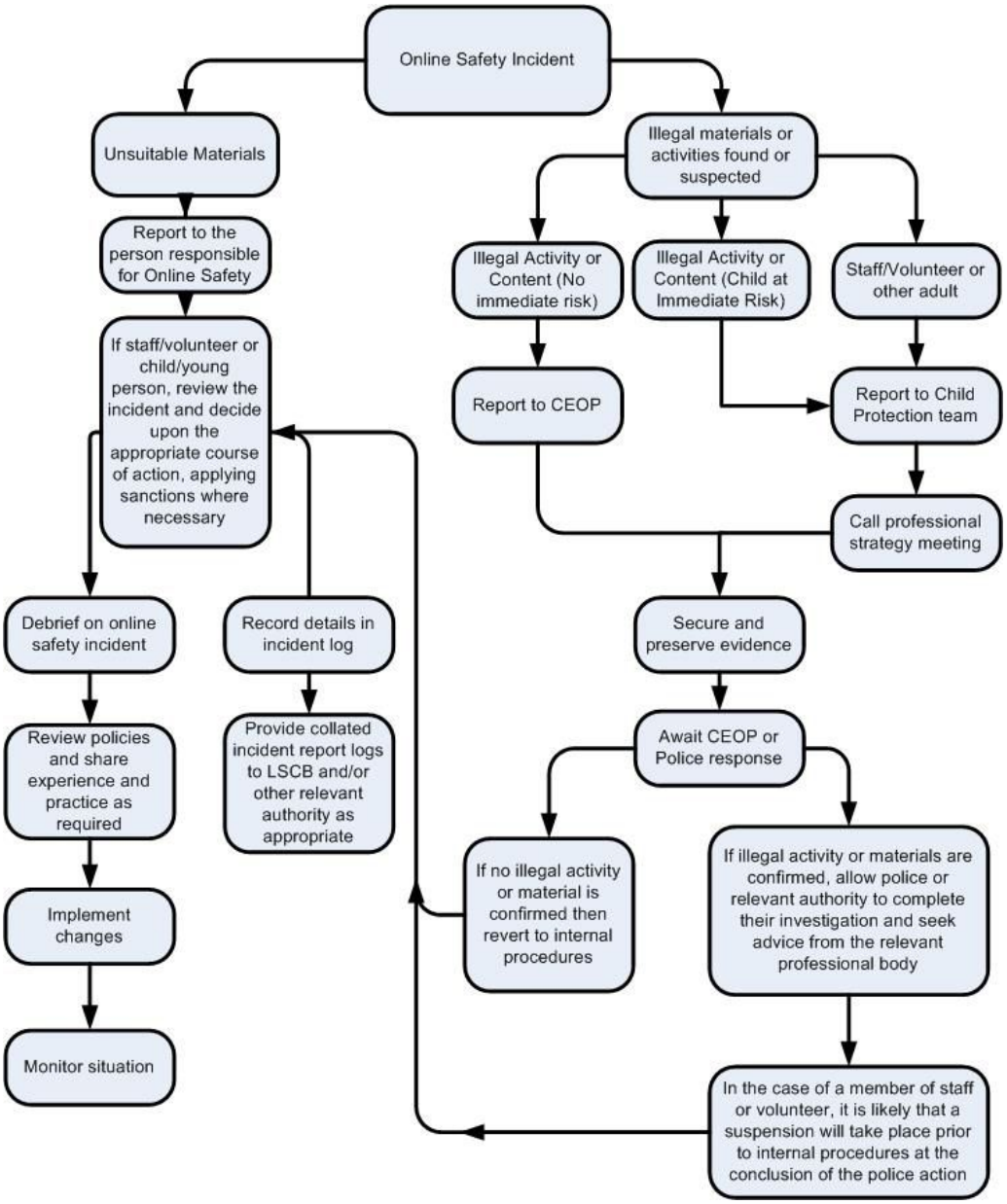
Any visitor can only access the schools network or internet with permission by an approved person because it involves the secure access keys and certificates. They should observe all elements of this policy and will not take any pictures, video or audio clips without first clearing this with the school eSafety Lead or a member of the Senior Leadership Team.

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, refer to the right hand side of the Flowchart below (appendix 1) 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 policy however, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

Where possible, 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

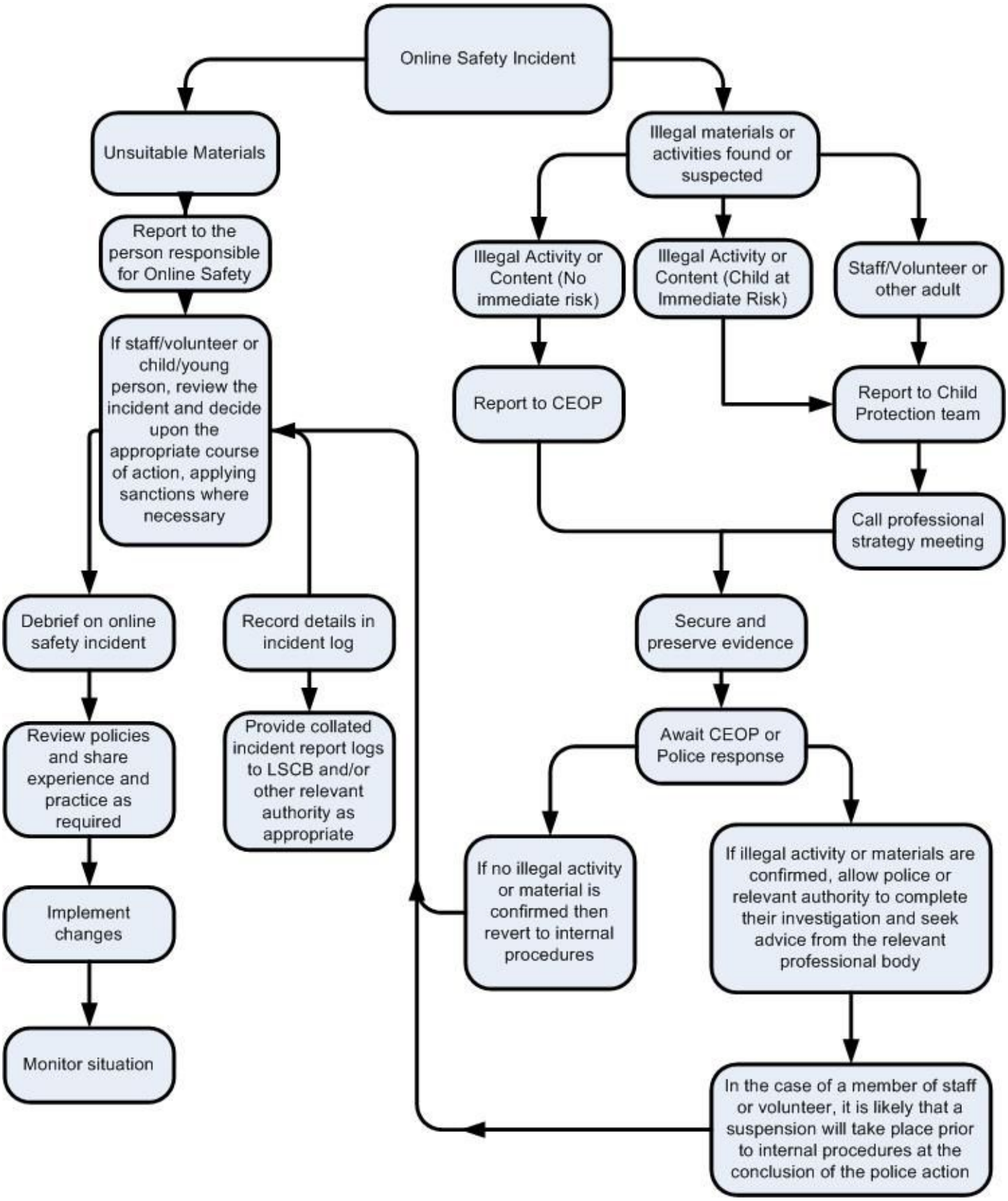
Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail and demonstrate that visits to these sites were carried out for child protection purposes. Evidence of this should be retained safely and confidentially by the group for reference purposes.

General Concerns or Complaints from External Sources

Any concerns or complaints can be directed by emailing the school to admin@njsch.uk marked "*FAO: eSafety Lead"* or through following the schools Complaints Procedure.

Appendix 1: Responding to incidents of misuse



Appendix 2 - Staff and Governor Acceptable Use Agreement

As an employee or governor of the school, you are bound to abide by the conditions in the eSafety policy and the acceptable use as follows. All are made aware of this policy upon their induction and are responsible for reading it.

1. Aims & Background

This ICT user agreement covers the use of all digital technologies while in school: ie email, internet, intranet, network resources, learning platform, software, communication tools, social networking tools, school website, apps and other relevant digital systems provided by the school or other information or systems processors.

This ICT user agreement also covers school issued equipment when used outside of school, use of online systems provided by the school such as VPN or webmail, or other systems providers when accessed from outside school.

This ICT user agreement also covers posts made on any non-school official social media platform or app, made from outside the school premises or school hours which reference the school or which might bring staff members or governors professional status into disrepute.

2. User Requirements

School employees, governors, and third party staff using school systems must comply with the requirements below. Failure to do so could possibly mean disciplinary procedures.

Please note that school systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. Your behaviour online when in school and on all school devices whether in school or otherwise may be subject to monitoring.

A. I will only use the school's resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body in the line of my employment.

B. I will set strong passwords, following advice provided by the school. I will change it frequently and I will not reveal my password(s) to anyone.

C. I will not use anyone else's password if they reveal it to me and will advise them to change it.

D. I will not allow unauthorised individuals to access email / internet / intranet / network / social networks / mobile apps / or any other system I have access to via the school or other authority or processing system.

E. I will ensure all documents, data, etc. are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols, and retention policy.

F. I will not engage in any online activity that may compromise my professional responsibilities.

G. I will only use the schools approved email system(s) for any school business.

H. I will only use the approved method/s of communicating with pupils or parents and will only communicate with them in a professional manner and on appropriate school business.

I. I will not support or promote extremist organisations, messages or individuals nor will I give a voice or opportunity to extremist visitors with extremist views.

J. I will not browse, download or send material that is considered offensive or of an extremist

nature by the school.

K. I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the Head.

L. I will not download any software or resources from the internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed. I will seek advice from the School Office.

M. I will not connect any device (including USB flash drive), to the network that does not have up-to- date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus and other malware systems.

N. I will not use images or videos of pupils or staff for any reason other than those expressly outlined by the school

O. I will only take or publish images of staff and students with their permission and in accordance with the school's consent guidelines. Images published on the school website, online learning en

P. vironment etc. will not identify students by name, or other personal information.

Q. I will use the school's Learning Platform or online cloud storage service in accordance with school protocols.

R. I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my professional role, and will create a distinction between the two.

S. I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.

T. I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.

U. I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

V. I will not store any pupil data that is not in line with the school's data policy and adequately protected. The school's data protection officer must be aware of all data storage.

W. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the relevant Senior Member of Staff / Designated Safeguarding Lead.

X. I understand that I have a responsibility to uphold the standing of the teaching profession and of the school, and that my digital behaviour can influence this.

Appendix 3: Acceptable Use Agreement for NJS Pupils

As a pupil of the school, you are bound to abide by the conditions in the eSafety policy and the acceptable use as follows. All parties are made aware of this policy at an appropriate level upon their induction and this is reinforced through our school curriculum. We have a wide range of measures in place to protect our children however, there is still the need to remain vigilant and follow the essential rules and guidelines outlined in this Agreement.

1. Aims & Background

This user agreement covers the use of all digital technologies while in school: ie email, internet, intranet, network resources, learning platform, software, communication tools, social networking tools, school website, apps and other relevant digital systems provided by the school or other information or systems processors.

This user agreement also covers school issued equipment when used outside of school, use of online systems provided by the school such as Gsuite, Gmail, or other systems providers when accessed from outside school. It also covers posts made on any non-school official social media platform or app, made from outside the school premises or school hours which reference the school or which might bring the professional status of the school into disrepute.

2. User Requirements

Pupils using school systems must comply with the requirements below. Failure to do so could possibly mean disciplinary procedures or even exclusion.

Please note that school systems and pupils are protected and monitored by security and filtering services to provide safe access to digital technologies. Your behaviour online when in school and on all school devices whether in school or otherwise may be subject to monitoring.

As a pupil, I agree that:

A. I will use the school computers and technology sensibly

B. I will ask permission from an adult before I use a device or the internet

C. I will only log on using my own username and password which I will keep confidential

D. I will only look at my own work and not delete anyone else's files

E. I will not bring in a USB devices from home without permission from a teacher

F. I will only email people I know from school using my school email account

G. I will always be polite and use appropriate language when emailing or sending messages on the computer

H. I will not give out my personal information or arrange to meet anyone

I. If I think anything on the internet upsets me or a stranger sends me a message, I will tell an adult

J. I know school will check my computer and be able to see what I am doing and what sites I have visited

K. If I break these rules I know I may be stopped from using the internet and/or computers or in extreme cases, could face exclusion or a lesser sanction