WOODLANDS
PRIMARY AND NURSERY SCHOOL

E-Safety Policy
(Including Safe Use of Technology)

Linked policies:

- Anti-Bullying Policy
- Appropriate use of Social Media Policy for Parents
- Alternative and off-site Provision Policy
- Behaviour and Discipline Policy
- Child Acceptable Use Policy
- Child on Child Abuse Policy
- Child Protection and Safeguarding Policy
- Drugs and Substance Abuse Policy
- Educational Visits Policy
- E-Safety Use of Devices Policy
- First Aid Policy
- Intimate Care Policy
- KCSIE 2023
- Managing Safeguarding Concerns and Allegations
- Safer Recruitment Policy
- Whistleblowing Policy

Date: September 2023

Review Date: September 2025

1. Introduction Writing and reviewing the e-safety policy

The e-Safety Policy relates to other policies including those for computing, bullying, behaviour and for child protection. All members of the senior leadership team, designated safeguarding leads and the computing subject leaders, have been tasked with ensuring the efficacy of this policy. There is also a designated link governor for E-safety (see Safeguarding Policy). The designated safeguarding lead takes lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place).

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties: the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements

2. Why Internet use is important

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. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. It is used to raise the standards of education, support professional work of staff and enhance the schools management and promote pupil achievement.

Current and emerging Internet and online technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet – World Wide Web
- E-mail
- Instant messaging (often using simple web cams) e.g. Instant Messenger)
- Web based voice and video calling (e.g. Skype, facetime)
- Online chat rooms
- Online discussion forums
- Social networking sites and apps(e.g. Facebook, Whatsapp, Snapchat)
- Blogs and Micro-blogs (e.g. Twitter)
- Podcasting (radio / audio broadcasts downloaded to devices)
- Video broadcasting sites (e.g. You Tube)
- Music and video downloading (e.g. iTunes)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, messaging, apps and internet access

Our whole school approach to the safe use of ICT

KCSIE groups online safety risks into 4 areas, content, contact, conduct and commerce:
Content is anything posted online - it might be words or it could be images and video. Children and young people may see illegal, inappropriate or harmful content when online. This includes things like pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact is about the risk of harm young people may face when interacting with other users online. This includes things like peer-to-peer pressure or seeing inappropriate commercial advertising.

Sometimes adults pose as children or young adults with the intention of grooming or exploiting a child or young person for sexual, criminal, financial or other purposes.

Conduct means the way people behave online. Some online behaviour can increase the likelihood, or even cause, harm - for example, online bullying. Conduct also includes things like sharing or receiving nudes and semi-nude images and viewing or sending pornography.

Commerce is about the risk from things like online gambling, inappropriate advertising, phishing or financial scams. Children and young people may be exposed to these risks directly. Schools should also consider how the risk from commerce applies to staff.

The 4c's of online safety provide schools with a framework to recognise and manage risk. At Woodlands, Computing Subject leaders work with DSLs and the Local Authority Safeguarding Team to produce a risk assessment, annually, to protect children and respond appropriately to concerns around these 4 areas.

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities
- E-Safety teaching is embedded into the school curriculum and schemes of work

3. Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors and DSL's, aims to embed safe practices into the culture of the school.

Leadership team

The senior leadership team ensures that the Policy is implemented across the school via the usual school monitoring procedures, including pupil voice. The SLT have a duty of care for ensuring the safety (including e-safety) of members of the school community, they are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

Governors

The School Governing body is responsible for overseeing and reviewing all school policies, including the e-Safety Policy.

E-Safety Coordinator / Officers:

The school has appointed Designated Safeguarding Leads encompassed within this role is a day-to-day responsibility for e-safety. This role includes:

- taking day to day responsibility for e-safety issues and 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
- liaising with the Local Authority / relevant body
- liaising with school technical staff
- receiving reports of e-safety incidents and creates a log of incidents to inform future e-safety developments, (Examples of suitable log sheets may be found later in this document).

- attending relevant meeting / committee of Governors / Directors
- reporting regularly to Senior Leadership Team

Network Manager / Technical staff:

Woodlands utilise Telford and Wrekin ICT support to ensure:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school / academy policies

School Staff

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.
Staff ensure they are familiar with the school e-Safety policy, and ask for clarification where needed. Class teachers ensure that pupils are aware of the e-Safety rules, introducing them at the beginning of each new school year and embedding them throughout the daily curriculum. All staff are responsible for ensuring that:

- they have an up-to-date awareness of e-safety matters and of the current school / academy e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Headteacher/SLT 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 (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and those processes are in place for dealing with any unsuitable material

that is found in internet searches

Pupils

Pupils are expected to take an active part in planned lessons and activities to support their understanding and confidence in dealing with e-Safety issues, both at home and school.
They are asked to agree to a set of guidelines and rules covering their responsibilities when using ICT at school and sign to say they accept these.

Parents

If a safety issue has arisen with a particular group of children or year group, then communication is made with the relevant parents. Woodlands also share e-safety top tips/help leaflets via the school website and Class Dojo platform. 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 / VLE and on-line student / pupil records
- their children's personal devices in the school (where this is allowed)

4. Internet Use & Management

Within Telford and Wrekin, 'Senso' monitoring software is used throughout the authority and runs behind every software application. All users must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource. The software is designed to protect users and will alert the Headteacher and School Business Manager of any potential breaches of the internet use policy which are then investigated and appropriate action is undertaken. (Screenshots are taken by the software at any instance of violation to allow easy tracking of the site/words used/user and computer involved).

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor TAW can accept liability for the material accessed, or any consequences of Internet access.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. They will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials. At Key stage 2 children accessing the internet are closely monitored.

5. E-safety Education

Users are informed that network and Internet use is monitored and traced to the individual user. E-safety resources are used within school to teach children, across all key stages safe use of the internet that is appropriate to their ability and year group. These resources a regularly updated, as the Internet and use of the Internet is constantly evolving. Woodlands uses a range of materials including the CE-OP website which includes a series of child-friendly lessons specifically catered to and differentiated for each Key Stage/Year group to teach them about all elements of e-safety. Integrated into this is an annual safer internet day (February) dedicated to educating the children around the dangers surrounding internet/digital device use. This comprises of key stage assemblies (age-related) and is followed up by lessons to reinforce the messages. Other assemblies dedicated to e-safety are taught throughout the year, often by the Safeguarding Champions team.

Teachers follow objectives for their year group which have been outlined in the 'Educating for a Connected World' (https://www.gov.uk/government/publications/education-for-a-connected-world) Government document. The objectives can be met through e-safety lessons, safer internet day, Share Aware week, Healthy Lifestyles week and during life lessons. At our school e-safety is interwoven throughout the curriculum and everyday classroom life.

6. Using the Internet for learning

The Internet is now an invaluable resource for learning for all our pupils, and we use it across the curriculum both for researching information and a source of digital learning materials.

Using the Internet for learning is now a part of the Computing Curriculum. We teach all of our pupils how to find appropriate information on the Internet, and how to ensure as far as possible that they understand who has made this information available, and how accurate and truthful it is.

- Teachers carefully plan all Internet-based teaching to ensure that pupils are focused and using appropriate and relevant materials.
- Children are taught how to use search engines and how to evaluate Internet-based information as part of the ICT curriculum, and in other curriculum areas where necessary.
- They are taught how to recognise the difference between commercial and non-commercial web sites, and how to investigate the possible authors of web-based materials.
- They are taught how to carry out simple checks for bias and misinformation
- They are taught that web-based resources have similar copyright status as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them.

7. Teaching safe use of the Internet and ICT

We understand that it is crucial to teach pupils how to use the Internet safely, both at school and at home, and we use the Kidsmart safety code to support our teaching in this area: Kidsmart has been developed by the Childnet charity, and is endorsed by the DfES http://www.kidsmart.org.uk

The main aspects of this approach include the following five SMART tips:

- Safe - Staying safe involves being careful and not giving out your name, address, mobile phone no., school name or password to people online...
- Meeting someone you meet in cyberspace can be dangerous. Only do so with your parents'/carers' permission and then when they are present...
- Accepting e-mails or opening files from people you don't really know or trust can get you into trouble - they may contain viruses or nasty messages...
- Remember someone online may be lying and not be who they say they are. If you feel uncomfortable when chatting or messaging end the conversation...
- Tell your parent or carer if someone or something makes you feel uncomfortable or worried...

Suitable material

We encourage pupils to see the Internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. Where possible, and particularly with younger children, we provide pupils with suggestions for suitable sites across the curriculum, and staff always check the suitability of websites before suggesting them to children, or using them in teaching.

Non-Education materials

We believe it is better to support children in finding their way around the Internet with guidance and positive role modelling rather than restrict Internet use to strict curriculum based research. As well as Internet material directly related to the curriculum, we encourage children to visit appropriate entertainment and child-oriented activity sites that have interesting and relevant activities, games and information, in free time at out-of-school-hours provision, and at home.
There is a selection of links to such resources available from on the school website, and in the shared pupil folders on the school network.

Unsuitable material

Despite the best efforts of the LA and school staff, occasionally pupils may come cross something on the Internet that they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken.
The action will include:

1. Making a note of the website and any other websites linked to it.
2. Informing the ICT Administrator
3. Logging the incident
4. Discussion with the pupil (and their parent) about the incident, and how to avoid similar experiences in future.

8. E-mail

E-Mail is a valuable and stimulating method of communication that plays an important role in many aspects of our lives today. We believe it is important that our pupils understand the role of e-mail, and how to use it appropriately and effectively.

Pupils are taught not to reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission. They are encouraged to immediately tell a teacher if they receive offensive e-mail. The forwarding of chain letters is not permitted.

All children in school have access to their own Purple Mash account, where they can send and receive emails. This is controlled by their class teacher to ensure no inappropriate messages are sent.

9. Internet-enabled mobile phones and handheld devices

More and more young people have access to sophisticated new internet-enabled devices such as SMART mobile phones, tablets and games consoles.

It is important that whilst the school recognises the potential advantages these devices can offer, there are clear and enforceable rules for their use in school, particularly when they give access to the Internet, and allow pictures and information to be remotely posted to a website or weblog.

Pupils will be taught the legal and moral implications of posting photos and personal information from mobile phones to public websites etc. and how the data protection and privacy laws apply. Pupils are not allowed to have personal mobile phones or other similar devices in school. Parents may request that such devices are kept at the School Office for pupils who may need them on their journey to and from school.

Use of digital and video images

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

- When using digital images, staff 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 students / 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 students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Children 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 good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website (may be covered as part of the AUA signed by parents or carers at the start of the year - see Parents / Carers Acceptable Use Agreement in the appendix)
- Pupil's work can only be published with the permission of the student / pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive

- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data. Woodlands ensures that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (See Privacy Notice section in the appendix)
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

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

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Published content and the school web site

The contact details on the Web site are the school address, e-mail and telephone number. Staff or pupils' personal information is not published, however each class group have a Class Dojo in which the parents can email for communication with the teachers and teaching assistants. The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

10. Publishing pupil's images and work

Written permission from parents or carers is obtained before photographs of pupils are published on the school Web site. A log is kept of children who we do not have permission to use their photographs and this log is updated regularly. Pupils' full names will not be used anywhere on the Web site or Blog if prior consent has not been obtained, particularly in association with photographs. Pupils work may be published on the website.

11. Social networking and personal publishing

The school will block/filter access to social networking sites. Pupils will be advised never to give out personal details of any kind that may identify them or their location whilst on the internet at school or home. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. The Woodlands Safeguarding Team support obtaining pupil voice and educating children about safe internet use and the implications of e-safety when gaming or using social networking sites. 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 students / 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 /academy or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Managing emerging technologies

Emerging technologies are examined by Telford and Wrekin ICT support for educational benefit and a risk assessment will be carried out before use in school is allowed.

12. Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

All pupils are aware for the rules of using the internet safely and appropriately. Where a pupil is found to be using the internet inappropriately, then sanctions will be applied according to the nature of the incident:

Unsuitable material (e.g. online games, celebrity pictures, music downloads, sport websites etc)
- Initial warning from class teacher
- Banning from out of school hours Internet facilities
- Report to Headteacher

- Letter to parent/carer

Offensive material (e.g. pornographic images, racist, sexist or hate website or images etc.)

- Incident logged and reported to Head teacher
- Initial letter to parent/carer
- Removal of Internet privileges/username etc.
- Meeting with Parent/Carer to re-sign the home-school agreement
- Removal of Out of School Hours access to Internet

13. Handling e-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the Headteacher. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Whilst it is the duty of the school to ensure that every child in our care is safe, the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, means it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences as a result of accessing the Internet.

14. Use of the Internet and ICT resources by school staff The Internet

Our school understands that the Internet is a valuable resource for school staff. It provides a wealth of resources, teaching materials and information that teachers can use across the curriculum. It allows staff to share resources with other schools, and to engage in debate and discussion.

We are committed to encouraging and supporting our school staff to make the best use of the Internet and all the opportunities it offers to enhance our teaching and support learning.

Internet Availability

To enable staff to make full use of these important resources, the Internet is available in school to all staff for professional use. The school also provides a T&W user account that gives further access to specific resources, online tools and email.

ICT Equipment and Resources

The school also offers staff access to appropriate ICT equipment and resources, including computers, laptops, tablets, interactive whiteboards, data projectors, digital cameras, sound recorders, control and data logging equipment and a range of professional and curriculum software.

Professional use

Staff are expected to model appropriate ICT and Internet use at all times. This supports our commitment to encouraging safe and appropriate ICT and Internet use by our pupils both in school and at home.

Staff are also careful to consider inclusion and equalities issues when using ICT and the Internet, and to provide pupils with appropriate models to support the school Inclusion and Equal Opportunities policies.

Staff who need support or CPD in using ICT as part of their professional practice can ask for support from the computing Co-ordinator or the school's Technology support.

Personal use of the Internet and ICT resources

Some equipment (including laptops) is available for loan to staff, with permission from the Headteacher. The appropriate forms and agreements must be signed.

However, all staff must be aware of the school policy on using school Internet and ICT resources for personal use.

E-mail

We recognise that e-mail is a useful and efficient professional communication tool. To facilitate this, staff members will be given a school e-mail address and we ask staff to use it for all professional communication with colleagues, organisations, companies and other groups.

Staff are reminded that using this e-mail address means that they are representing the school, and all communications must reflect this.

E-mail accounts provided by the school may sometimes need to be accessed, although personal privacy will be respected.

Online discussion groups, bulletin boards and forums, online chat and messaging

We realise that a growing number of educationalists and education groups use discussion groups, online chat forums and bulletin board to share good practice and disseminate information and resources.

The use of online discussion groups and bulletin boards relating to professional practice and continuing professional development is encouraged, although staff are reminded that they are representing the school, and appropriate professional standards should apply to all postings and messages.

Social Networking

The school appreciates that many staff will use social networking sites and tools. The use of social networking tools and how it relates to the professional life of school staff is covered in Staff Professional Conduct expectations and agreements. As with discussion groups, staff are reminded that professional standards should apply to all postings and messages.

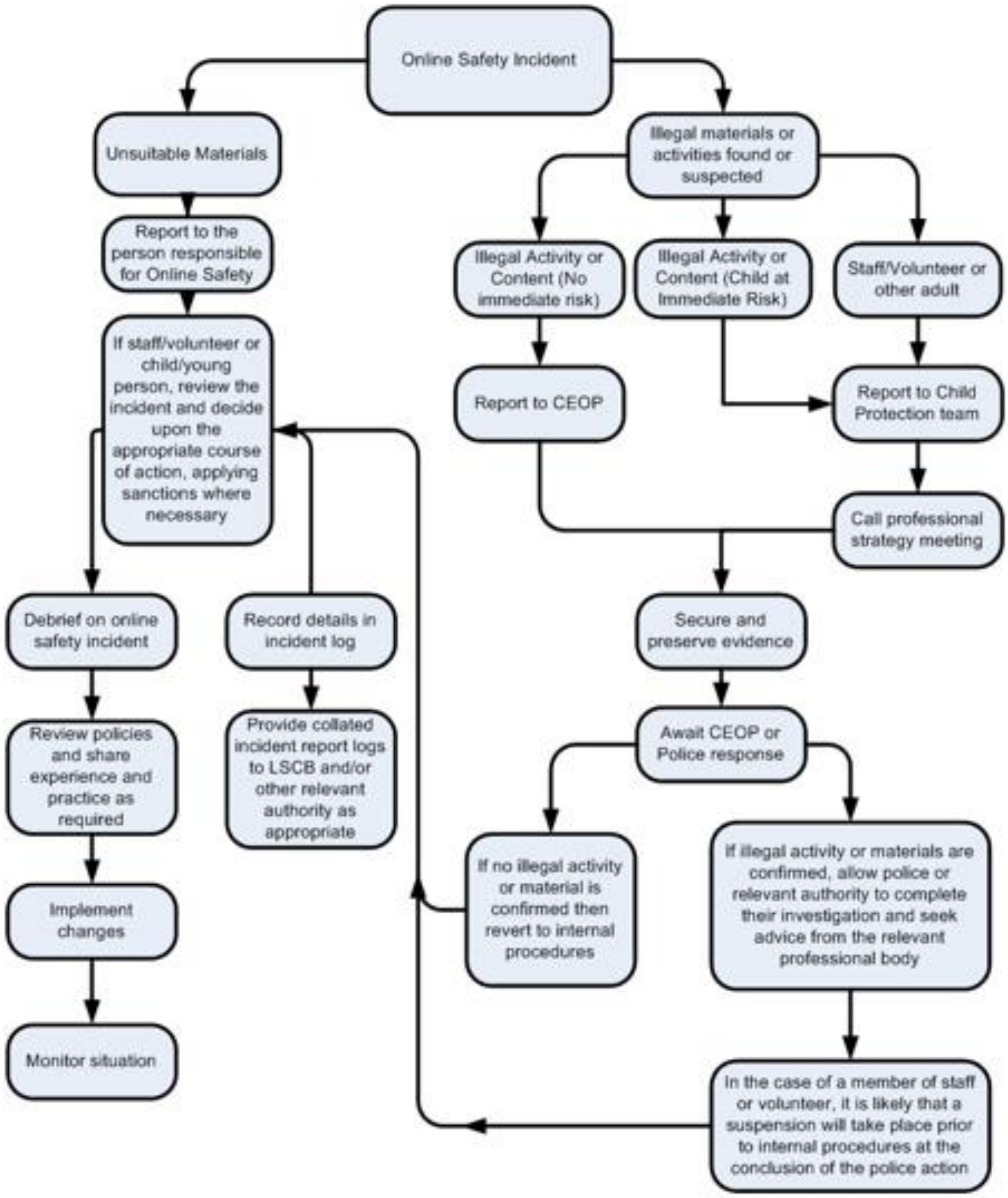
Data Protection and Copyright

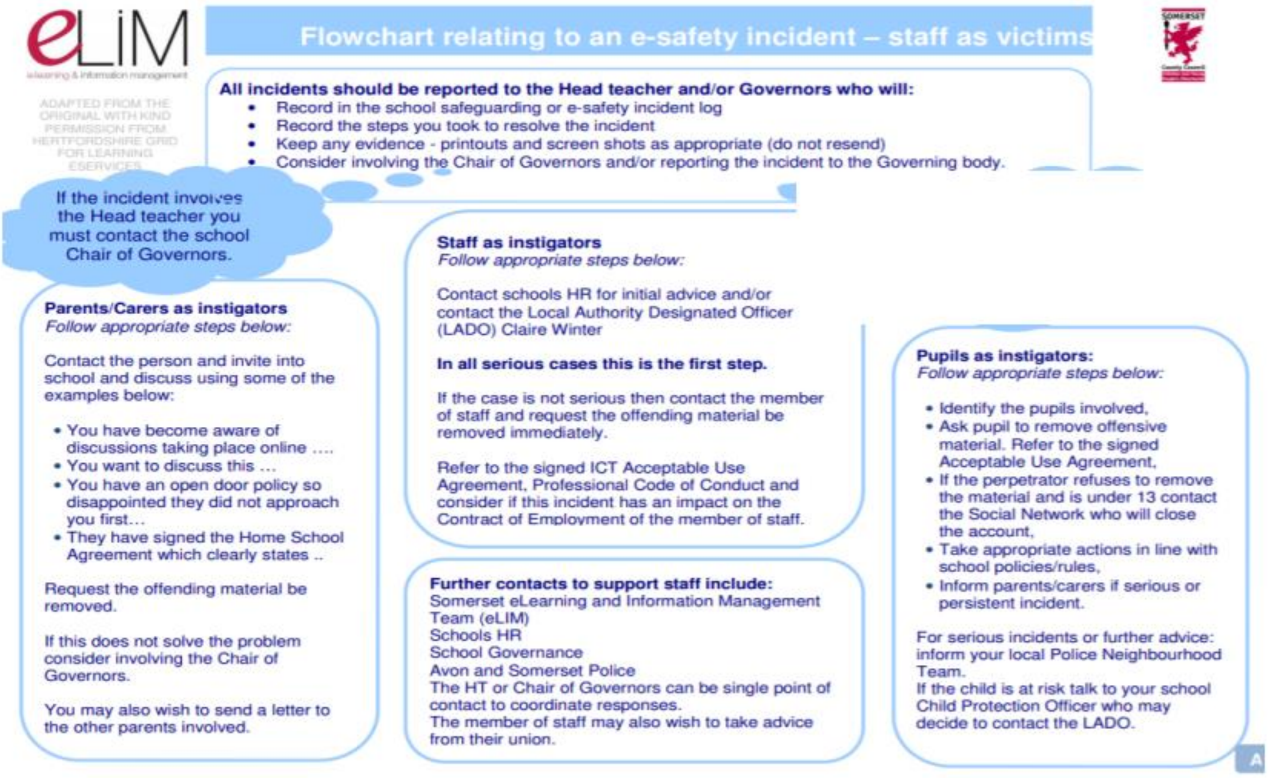
The school has data protection policy in place – please see separate documentation for more details.

Staff are aware of this policy, and how it relates to Internet and ICT use, in particular with regard to pupil data and photographs, and follow the guidelines as necessary.

Staff understand that there are complex copyright issues around many online resources and materials, and always give appropriate credit when using online materials or resources in teaching and learning materials. They also support pupils to do the same.

Supporting Flow Chart diagrams:


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action



Flowchart relating to an e-safety incident – staff as victims

eLiM e-learning & information management

ADAPTED FROM THE ORIGINAL WITH KIND PERMISSION FROM HERTFORDSHIRE GRID FOR LEARNING ESERVICES

All incidents should be reported to the Head teacher and/or Governors who will:

- Record in the school safeguarding or e-safety incident log
- Record the steps you took to resolve the incident
- Keep any evidence - printouts and screen shots as appropriate (do not resend)
- Consider involving the Chair of Governors and/or reporting the incident to the Governing body.

If the incident involves the Head teacher you must contact the school Chair of Governors.

Parents/Carers as instigators
Follow appropriate steps below:

Contact the person and invite into school and discuss using some of the examples below:

- You have become aware of discussions taking place online ….
- You want to discuss this …
- You have an open door policy so disappointed they did not approach you first…
- They have signed the Home School Agreement which clearly states ..

Request the offending material be removed.

If this does not solve the problem consider involving the Chair of Governors.

You may also wish to send a letter to the other parents involved.

Staff as instigators
Follow appropriate steps below:

Contact schools HR for initial advice and/or contact the Local Authority Designated Officer (LADO) Claire Winter

In all serious cases this is the first step.

If the case is not serious then contact the member of staff and request the offending material be removed immediately.

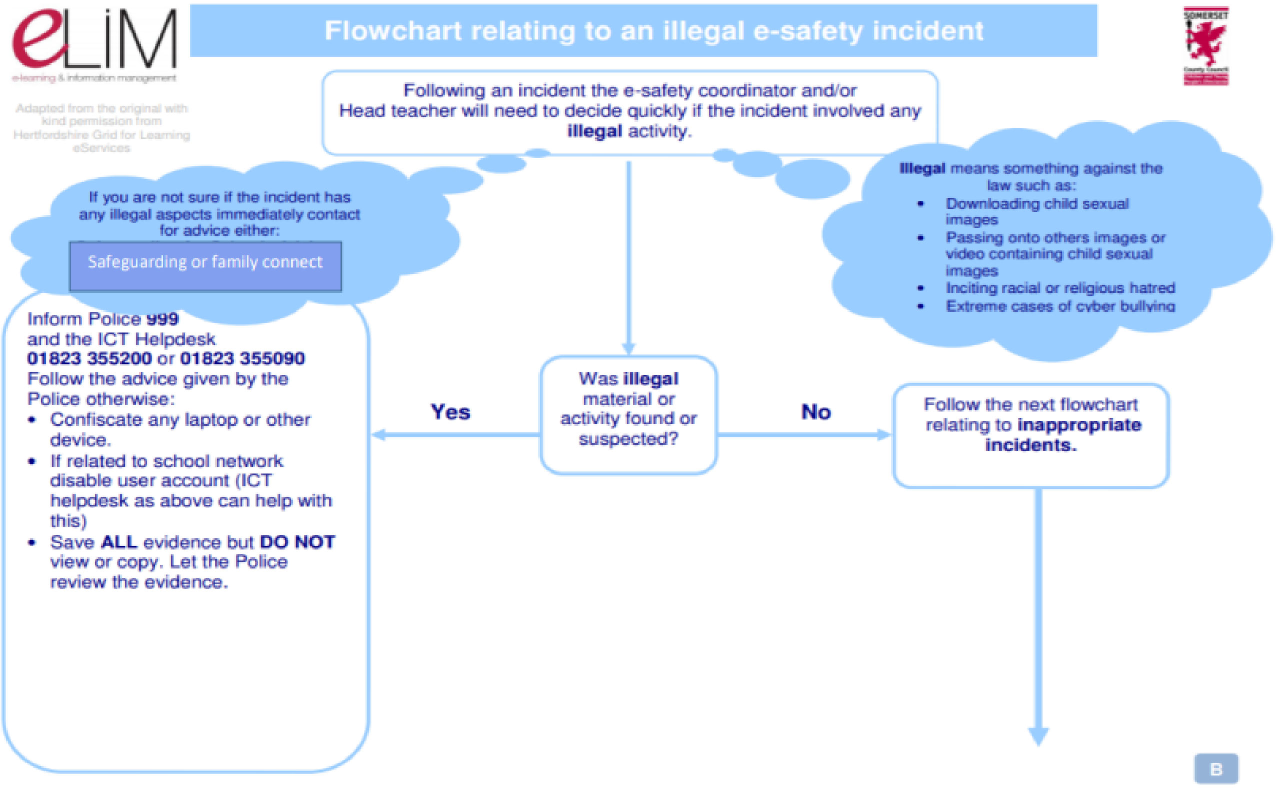
Refer to the signed ICT Acceptable Use Agreement, Professional Code of Conduct and consider if this incident has an impact on the Contract of Employment of the member of staff.

Further contacts to support staff include:
Somerset eLearning and Information Management Team (eLIM)
Schools HR
School Governance
Avon and Somerset Police
The HT or Chair of Governors can be single point of contact to coordinate responses.
The member of staff may also wish to take advice from their union.

Pupils as instigators:
Follow appropriate steps below:

- Identify the pupils involved,
- Ask pupil to remove offensive material. Refer to the signed Acceptable Use Agreement,
- If the perpetrator refuses to remove the material and is under 13 contact the Social Network who will close the account,
- Take appropriate actions in line with school policies/rules,
- Inform parents/carers if serious or persistent incident.

For serious incidents or further advice: inform your local Police Neighbourhood Team.
If the child is at risk talk to your school Child Protection Officer who may decide to contact the LADO.



Flowchart relating to an illegal e-safety incident

eLiM e-learning & information management

Adapted from the original with kind permission from Hertfordshire Grid for Learning eServices

Following an incident the e-safety coordinator and/or Head teacher will need to decide quickly if the incident involved any **illegal** activity.

If you are not sure if the incident has any illegal aspects immediately contact for advice either:

Safeguarding or family connect

Illegal means something against the law such as:

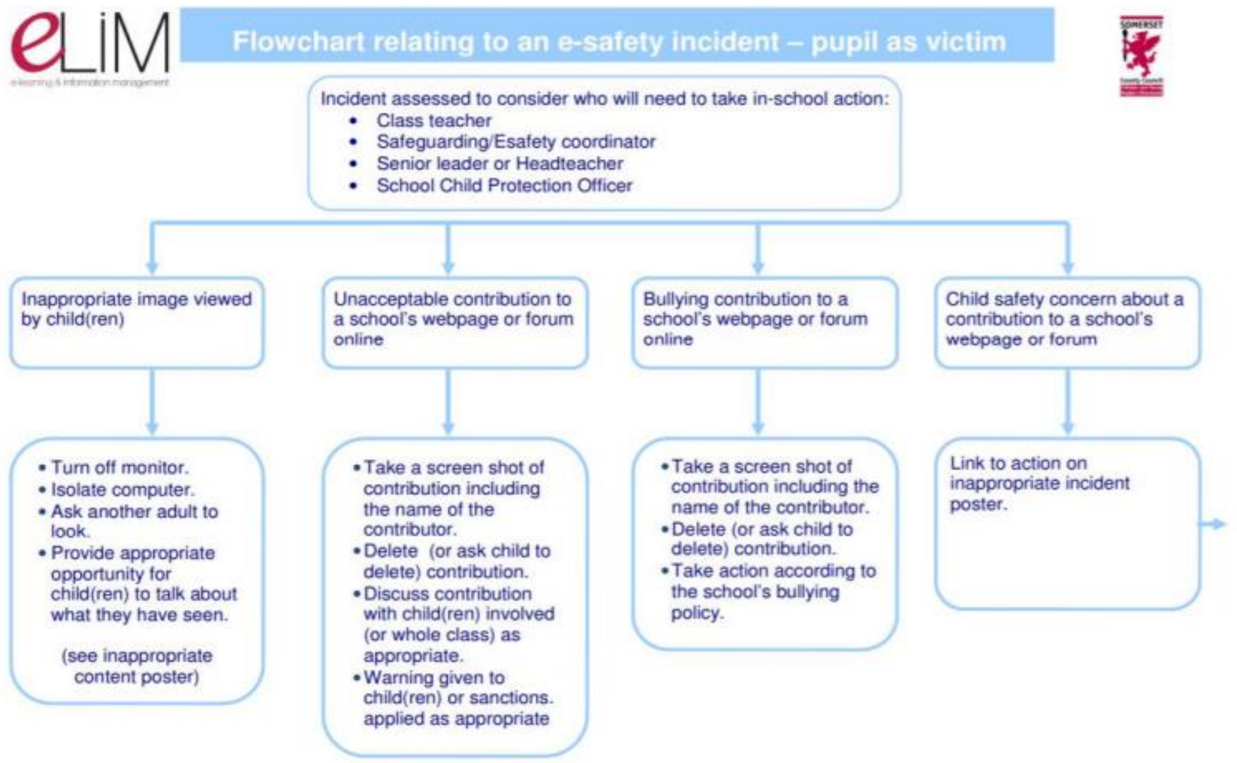
- Downloading child sexual images
- Passing onto others images or video containing child sexual images
- Inciting racial or religious hatred
- Extreme cases of cyber bullying

Was **illegal** material or activity found or suspected?

Inform Police **999** and the ICT Helpdesk **01823 355200** or **01823 355090** Follow the advice given by the Police otherwise:

- Confiscate any laptop or other device.
- If related to school network disable user account (ICT helpdesk as above can help with this)
- Save **ALL** evidence but **DO NOT** view or copy. Let the Police review the evidence.

Follow the next flowchart relating to **inappropriate incidents.**



Flowchart relating to an e-safety incident – pupil as victim

Incident assessed to consider who will need to take in-school action:

- Class teacher
- Safeguarding/Esafety coordinator
- Senior leader or Headteacher
- School Child Protection Officer

Inappropriate image viewed by child(ren)

- Turn off monitor.
- Isolate computer.
- Ask another adult to look.
- Provide appropriate opportunity for child(ren) to talk about what they have seen.

(see inappropriate content poster)

Unacceptable contribution to a school's webpage or forum online

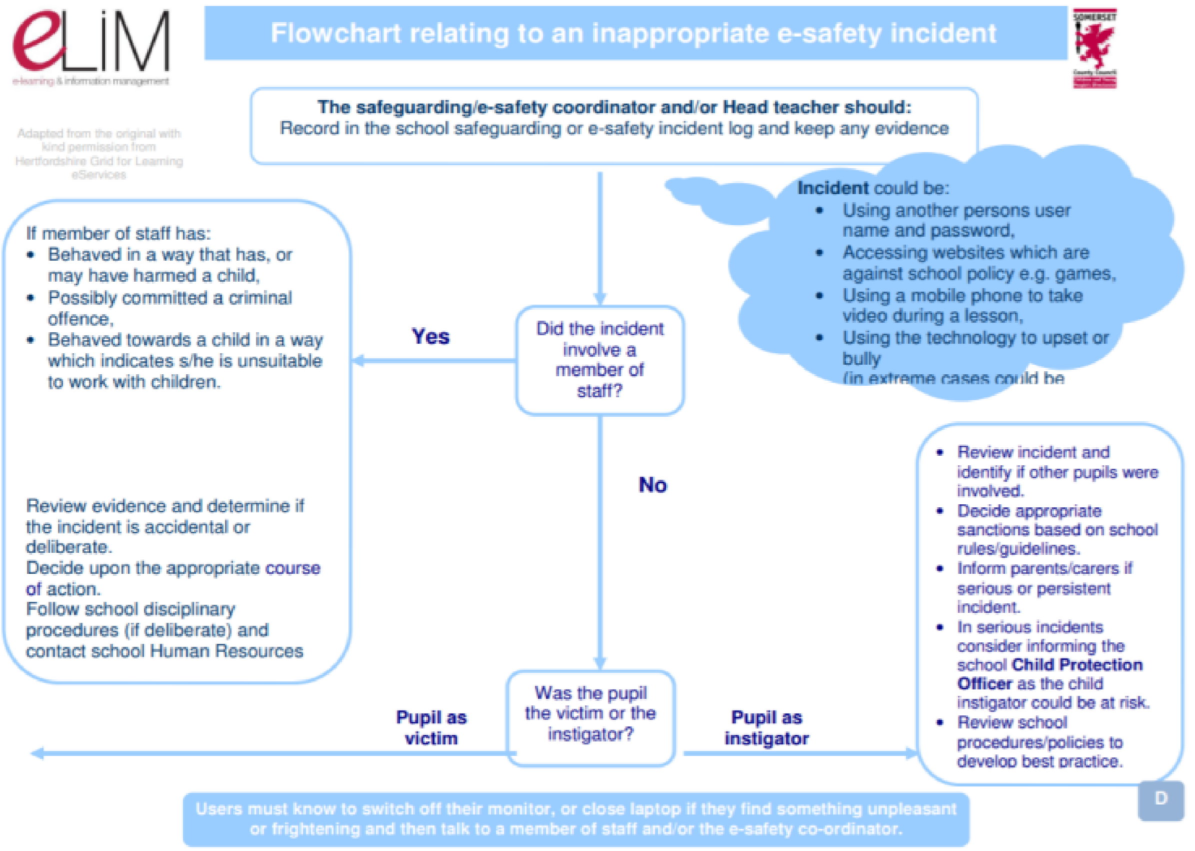
- Take a screen shot of contribution including the name of the contributor.
- Delete (or ask child to delete) contribution.
- Discuss contribution with child(ren) involved (or whole class) as appropriate.
- Warning given to child(ren) or sanctions. applied as appropriate

Bullying contribution to a school's webpage or forum online

- Take a screen shot of contribution including the name of the contributor.
- Delete (or ask child to delete) contribution.
- Take action according to the school's bullying policy.

Child safety concern about a contribution to a school's webpage or forum

Link to action on inappropriate incident poster.



Flowchart relating to an inappropriate e-safety incident

Adapted from the original with kind permission from Hertfordshire Grid for Learning eServices

The safeguarding/e-safety coordinator and/or Head teacher should:
Record in the school safeguarding or e-safety incident log and keep any evidence

Incident could be:

- Using another persons user name and password,
- Accessing websites which are against school policy e.g. games,
- Using a mobile phone to take video during a lesson,
- Using the technology to upset or bully
(in extreme cases could be

Did the incident involve a member of staff?

Yes

If member of staff has:

- Behaved in a way that has, or may have harmed a child,
- Possibly committed a criminal offence,
- Behaved towards a child in a way which indicates s/he is unsuitable to work with children.

Review evidence and determine if the incident is accidental or deliberate.
Decide upon the appropriate course of action.
Follow school disciplinary procedures (if deliberate) and contact school Human Resources

No

Was the pupil the victim or the instigator?

Pupil as victim

Pupil as instigator

- Review incident and identify if other pupils were involved.
- Decide appropriate sanctions based on school rules/guidelines.
- Inform parents/carers if serious or persistent incident.
- In serious incidents consider informing the school **Child Protection Officer** as the child instigator could be at risk.
- Review school procedures/policies to develop best practice.

D

Users must know to switch off their monitor, or close laptop if they find something unpleasant or frightening and then talk to a member of staff and/or the e-safety co-ordinator.