Athelstan Primary School

e-Safeguarding Policy

October 2024
Review October 2025

Contents

Introduction

This eSafety policy recognises the commitment of our school to eSafety and acknowledges its part in the school's overall Safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep pupils safe when using technology. We believe the whole school community can benefit from the opportunities provided by the Internet and other technologies used in everyday life. The eSafety policy supports this by identifying the risks and the steps we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities. We wish to ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where necessary, disciplinary or legal action will be taken. We aim to minimise the risk of misplaced or malicious allegations being made against adults who work with pupils.

Our expectations for responsible and appropriate conduct are formalised in our Acceptable Use Policies (AUP) which we expect all staff and pupils to follow.

As part of our commitment to eSafety we also recognize our obligation to implement a range of security measures to protect the school network and facilities from attack, compromise and inappropriate use and to protect school data and other information assets from loss or inappropriate use.

Scope of the Policy

- This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, work placement students, visitors, and community users) who have access to and are users of school ICT systems, both in and out of school.

- The school's behaviour policy will be applied to incidents of cyber-bullying and e-Safeguarding including incidents that may take place out of school where appropriate.

- The Education Act 2011 gives the school the power to confiscate and search the contents of any mobile device if the Headteacher believes it contains any illegal content or material that could be used to bully or harass others.

- The school will identify within this policy and in the associated behaviour and anti-bullying policies, how incidents will be managed and will, where known, inform parents/carers of incidents of inappropriate e-Safeguarding behaviour that take place out of school.

Schedule for Development / Monitoring / Review

Title	**E-Safeguarding Policy**
Date	*22/10/2024*
Author	*E-safety Team*
Monitoring will take place at regular intervals (at least annually):	*Annually*
The Governing Body will receive a report on the implementation of the policy including anonymous details of any e-Safeguarding incidents at regular intervals:	*Annually*
The Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*October 2025*
Should serious e-Safeguarding incidents take place, the following external persons / agencies should be informed:	*e-Safety Leader* *Safeguarding Officer* *Police and Commissions Officer*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys / questionnaires of students / pupils (including Every Child Matters Survey) /parents / carers / staff

Communication of the Policy

- The Athelstan Primary's senior leadership team will be responsible for ensuring all members of school staff and pupils are aware of the existence and contents of the school e-Safeguarding policy and the use of any new technology within school.
- All amendments will be published and awareness sessions will be held for all members of the school community.
- Any amendments will be discussed by the School Council to ensure the language and vocabulary is appropriate and understandable for the policy's intended audience.
- An e-Safeguarding or eSafety training programme will be established across the school to include a regular review of the e-Safeguarding policy.
- e-Safeguarding or eSafety training will be part of the transition programme across the Key Stages and when moving between establishments, pupils' responsibilities regarding the school e-Safeguarding policy will be reviewed.
- Pertinent points from the school e-Safeguarding policy will be reinforced across the curriculum and across all subject areas when using ICT equipment within school.
- The key messages contained within the e-Safeguarding policy will be reflected and consistent within all acceptable use policies in place within school.
- We endeavour to embed e-Safeguarding messages across the curriculum whenever the internet or related technologies are used.
- There will be an online safety display in school.

Roles and Responsibilities

We believe that e-Safeguarding is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Senior Leadership Team

- The Headteacher has overall responsibility for e-Safeguarding all members of the school community, though the day-to-day responsibility for e-Safeguarding will be delegated to the E-Safeguarding Leader and safeguarding team.

- The headteacher and senior leadership team are responsible for ensuring that the E-Safeguarding leader and other relevant staff receive suitable training to enable them to carry out their e-Safeguarding roles and to train other colleagues when necessary.

- The headteacher and senior leadership team will ensure that there is a mechanism in place to allow for monitoring and support of those in school who carry out the internal e-Safeguarding monitoring role. This provision provides a safety net and also supports those colleagues who take on important monitoring roles.

- The senior leadership team and governors can request monitoring reports from the e-Safeguarding leader and safeguarding team.

- The headteacher and senior leadership team should ensure that they are aware of procedures to be followed in the event of a serious e-Safeguarding incident.

Responsibilities of the e-Safeguarding Team

- To ensure that the school e-Safeguarding policy is current and pertinent.
- To ensure that the school e-Safeguarding policy is systematically reviewed at agreed time intervals.
- To ensure that school Acceptable Use Policies are appropriate for the intended audience.
- To promote to all members of the school community the safe use of the internet and any technologies deployed within school.

Responsibilities of the e-Safeguarding Leader/Team

- To promote an awareness and commitment to e-Safeguarding throughout the school.
- To be the first point of contact in school on all e-Safeguarding matters.
- To take day-to-day responsibility for e-Safeguarding within school and to have a leading role in establishing and reviewing the school e-Safeguarding policies and procedures.
- To lead the school e-Safeguarding group or committee.
- To have regular contact with other e-Safeguarding committees, e.g. Safeguarding Children Board.
- To communicate regularly with school technical staff.

- To communicate regularly with the designated e-Safeguarding governor.
- To communicate regularly with the senior leadership team.
- To create and maintain e-Safeguarding policies and procedures.
- To develop an understanding of current e-Safeguarding issues, guidance and appropriate legislation.
- To ensure that all members of staff receive an appropriate level of training in e-Safeguarding issues.
- To ensure that e-Safeguarding education is embedded across the curriculum.
- To ensure that e-Safeguarding is promoted to parents and carers.
- To liaise with the local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate.
- To monitor and report on e-Safeguarding issues to the e-Safeguarding group and the senior leadership team as appropriate.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safeguarding incident.
- To ensure that an e-Safeguarding incident log is kept up to date.

Responsibilities of the Teaching and Support Staff

- To teach e-safety as well as model it through lessons as a unit (National Online Safety website unit and RSHE unit) or a discrete session.
- To read, understand and help promote the school's e-Safeguarding policies and guidance including the school staff Acceptable Use Policy.
- To report any suspected misuse or problem to the e-Safeguarding coordinator.
- To develop and maintain an awareness of current e-Safeguarding issues and guidance.
- To model safe and responsible behaviours in their own use of technology and to supervise and guide pupils carefully when engaged in learning activities involving technology.
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones etc.
- To embed e-Safeguarding messages in learning activities across all areas of the curriculum including research skills and legal issues relating to electronic content such as copyright laws.
- To be aware of e-Safeguarding issues related to the use of mobile phones, cameras and handheld devices.
- To understand and be aware of incident-reporting mechanisms that exist within the school.
- Ensure that sensitive and personal data is kept secure at all times by using encrypted data storage and by transferring data through secure communication systems.

Responsibilities of Technical Staff

- To read, understand, contribute to and help promote the school's e-Safeguarding policies and guidance including the school staff Acceptable Use Policy.
- To report any e-Safeguarding related issues that come to your attention to the e-Safeguarding coordinator.

- To develop and maintain an awareness of current e-Safeguarding issues, legislation and guidance relevant to their work.
- To maintain a professional level of conduct in your personal use of technology at all times.
- To support the school in providing a safe technical infrastructure to support learning and teaching.
- To ensure that access to the school network is only through an authorised, restricted mechanism.
- To ensure that provision exists for misuse detection and malicious attack.
- To take responsibility for the security of the school ICT system.
- To liaise with the local authority and other appropriate people and organisations on technical issues.
- To document all technical procedures and review them for accuracy at appropriate intervals.
- To restrict all administrator level accounts appropriately.
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices.
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school.
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To ensure that controls and procedures exist so that access to school-owned software assets is restricted.

Protecting the professional identity of all staff, work placement students and volunteers

Communication between adults and between children / young people and adults, by whatever method, should be transparent and take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, text messaging, social networks, e-mails, digital cameras, videos, web-cams, websites, forums and blogs.

When using digital communications, staff and volunteers should:

- Only make contact with children and young people for professional reasons and in accordance with the policies and professional guidance of the school.
- Not share any personal information with a child or young person e.g. should not give their personal contact details to children and young people including email, home or mobile telephone numbers.
- Not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm.
- Not send or accept a friend request from the child/young person on social networks.
- Not send or accept a friend request from a former student, under the age of 18 years, on social networks.
- Be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.
- Ensure that all communications are transparent and open to scrutiny.

- Be careful in their communications with children so as to avoid any possible misinterpretation.
- Ensure that if they have a personal social networking profile, details are not shared with children and young people in their care (making every effort to keep personal and professional online lives separate).
- Not post information online that could bring the school into disrepute.
- Be aware of the sanctions that may be applied for breaches of policy related to professional conduct.

Responsibilities of the Child Protection Officer

- To understand the issues surrounding the sharing of personal or sensitive information.
- To understand the dangers regarding access to inappropriate online contact with adults and strangers.
- To be aware of potential or actual incidents involving grooming of young children.
- To be aware of and understand cyberbullying and the use of social media for this purpose.

Responsibilities of Pupils

- To read, understand and adhere to the school pupil Acceptable Use Policy.
- To help and support the school in the creation of e-Safeguarding policies and practices and to adhere to any policies and practises the school creates.
- To know and understand school policies on the use of mobile phones, digital cameras and handheld devices.
- To know and understand school policies regarding cyberbullying.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home.
- To be fully aware of research skills and of legal issues relating to electronic content such as copyright laws.
- To take responsibility for each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used outside school.
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within school.
- To discuss e-Safeguarding issues with family and friends in an open and honest way.

Responsibilities of Parents / Carers

- To help and support the school in promoting e-Safeguarding.
- To read, understand and promote the school pupil Acceptable Use Policy with their children.

- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home.
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- To discuss e-Safeguarding concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology.
- To model safe and responsible behaviours in their own use of technology
- To consult with the school if they have any concerns about their children's use of technology.
- To agree to and sign the home-school agreement which clearly sets out the use of photographic and video images outside of school.

Responsibilities of the Governing Body

- To read, understand, contribute to and help promote the school's e-Safeguarding policies and guidance.
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils.
- To develop an overview of how the school ICT infrastructure provides safe access to the internet.
- To develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
- To support the work of the e-Safeguarding group in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in e-Safeguarding activities.
- To ensure appropriate funding and resources are available for the school to implement its e-Safeguarding strategy.

The role of the E-Safety Governor includes:

- meetings with the E-Safety Leader
- monitoring of e-safety incident logs
- reporting to Governors meeting as requested

Responsibilities of Other Community/ External Users

- The school will liaise with local organisations to establish a common approach to e-Safeguarding and the safe use of technologies.
- The school will be sensitive and show empathy to internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice where appropriate.
- Any external organisations will sign an Acceptable Use Policy prior to using any equipment or the internet within school.
- The school will provide an Acceptable Use Policy for any guest who needs to access the school computer system or internet on school grounds.
- The school will ensure that appropriate levels of supervision exist when external organisations make use of the internet and ICT equipment within school.

Education

Pupils

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

E-Safety education will be provided in the following ways:

- e-Safeguarding related lessons following the National Online Safety website curriculum, assemblies and whole-school activities are held in every year group as part of the Online Safety and RSHE curriculum including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant e-Safeguarding messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind pupils about their responsibilities through an Acceptable Use Policy which every pupil will sign and which will be displayed throughout the school.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- All pupils will be taught in an age-appropriate way about copyright in relation to online resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the internet.
- Pupils will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

All Staff (including Governors)

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

- A planned programme of formal e-safety training will be made available to staff through the National Online Safety website.
- Staff will be kept up to date with current, relevant updates through emails and staff training.
- An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.
- This e-Safeguarding policy and its updates will be presented to and discussed by staff in staff meetings.
- The E-Safety Leader (or other nominated person) will provide advice/guidance/ training as required to individuals as required.

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 and in promoting the positive use of the internet and social media. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through:

- newsletters
- letters
- website / VLE / twitter and Squid
- information about national / local e-safety campaigns / literature

Use of digital and video images

- 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.

- Staff 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. Permissions for images should be checked before images are taken.

- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Pupils must not take, use, share, publish or distribute images of others without their permission.

- Photographs published on the website, or elsewhere that include 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 pupils are published on the school website.

- Pupil's work can only be published with the permission of the pupil and parents or carers.

- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

Managing ICT systems and access

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- All access to school ICT systems should be based upon a 'least privilege' approach.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- The school will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive. All pupils will be given an individual google account and password, so they can access Google Classroom . These will be kept secure, in line with the pupil Acceptable Use Policy. They will ensure they log out after each session.
- Members of staff will access the internet using an individual id and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their id and password. They will abide by the school AUP at all times.

Filtering internet access

- The school uses a filtered internet service. The filtering system is provided by Yorkshire and Humberside Grid for Learning.
- The school's internet provision will include filtering appropriate to the age and maturity of pupils.
- The school will always be proactive regarding the nature of content which can be viewed through the school's internet provision.
- The school will have a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the e-Safeguarding Leader. All incidents should be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the e-Safeguarding Coordinator. The school will report such incidents to appropriate agencies including the filtering provider, the local authority, CEOP or the IWF.
- The school will regularly review the filtering product for its effectiveness.
- The school filtering system will block all sites on the Internet Watch Foundation list and this will be updated daily.
- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked.
- Pupils will be taught to assess content as their internet usage skills develop.
- Pupils will use age-appropriate tools to research internet content.

- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Passwords

- A secure and robust username and password convention exists for all system access. (email, network access, school management information system).
- Pupils will have a generic 'year group pupil' login to all school ICT equipment.
- All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- All information systems require end users to change their password at first log on.
- Users should be prompted to change their passwords at prearranged intervals or at any time that they feel their password may have been compromised.
- Users should change their passwords whenever there is any indication of possible system or password compromise
- All staff and pupils have a responsibility for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- All staff and pupils will have appropriate awareness training on protecting access to their personal username and passwords for ICT access.
- All staff and pupils will sign an Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to username and passwords.
- Do not write down system passwords.
- Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
- Always use your own personal passwords to access computer based services, never share these with other users.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Never save system-based usernames and passwords within an internet browser.
- All access to school information assets will be controlled via username and password.
- No user should be able to access another user's files unless delegated permission has been granted.
- Access to personal data is securely controlled in line with the school's personal data policy.
- The school maintains a log of all accesses by users and of their activities while using the system.
- Passwords should contain a minimum of eight characters and be difficult to guess.
- Users should create different passwords for different accounts and applications.
- Users should use numbers, letters and special characters in their passwords (! @ # $ % * ( ) - + = , < > : : " '): the more randomly they are placed, the more secure they are.

Management of assets

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007 and /or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2013

Data Protection

Personal Data

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.
- At all times take care to ensure the safekeeping 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 or their computer is locked when left unattended.
- Transfer data using encryption and secure password protected devices.
- When personal data is stored on any portable computer system, USB stick or any other removable media:

    - the data must be encrypted and password protected
    - the device must be password protected
    - the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

- The school has established an information-handling procedure and assessed the risks involved with handling and controlling access to all levels of information within school.
- The school has deployed appropriate technical controls to minimise the risk of data loss or breaches.
- All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- All access to information systems should be controlled via a suitably complex password.
- Any access to personal and sensitive information should be assessed and granted by the SIRO and the applicable IAO.
- All access to the school information management system will be on a need-to-know or least privilege basis. All access should be granted through the SIRO or IAO.
- All information on school servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know/ least privilege basis. All access should be granted through the SIRO or IAO.
- Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school.
- All physical information will be stored in controlled access areas.

- All communications involving personal or sensitive information (email, fax or post) should be appropriately secured.
- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.

Secure Transfer Process

Email

- It is advisable not to use public email accounts for sending and receiving sensitive or personal data.

- All work-related emails are carried out using the school's email system.

- **DO NOT** include personal or sensitive information within the email itself, as the information sent should be by a secure method. This can be done by creating a document (e.g. Word document) and then encrypting the document and sending it as an attachment with the email.

- Encryption makes a file non-readable to anyone who does not have the password to open it, therefore, it reduces the risk of unauthorised people having access to the information and protects staff from breaching the law.

FAX

- Fax machines will be situated within controlled areas of the school.

- All sensitive information or personal data sent by email or fax will be transferred using a secure method.

- Personal or sensitive information must be within the email itself as the information may be insecure. This can be done by creating a document (e.g. Word document) and then encrypting the document and sending it as an attachment with the email.

Communication Technologies

A wide range of rapidly developing communications technologies has the potential to enhance learning.

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school (Pupils hand into class teacher who secures them in a locked cupboard, staff to have them on silent & locked away during class time)	X				X			
Smartwatches may be brought to school (not encouraged) but pupils hand them to class teacher who secures them in a locked cupboard, staff to have them on silent & locked away during class time.	X				X			
Use of mobile phones in lessons				X				X
Use of mobile phones in social time		X						X
Use of smart watches in social time		X						X
Use of smart watches in lesson time				X				X
Taking photos on mobile phones or other camera devices		X						X
Use of hand held devices eg PDAs, PSPs, IPads		X				X		
Use of personal email addresses in school, or on school network		X						X
Use of school email for personal emails				X				X
Use of chat rooms / facilities at school				X				X
Use of instant messaging		X						X
Use of social networking sites – LA approved ones only		X					X	
Use of blogs		X					X	

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

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to

communicate with others when in school, or on school systems (e.g. by remote access).

- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents/carers (email, chat, VLE etc) must be professional in tone and content.

Unsuitable / inappropriate activities

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for certain users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					✔
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					✔
	adult material that potentially breaches the Obscene Publications Act in the UK					✔
	criminally racist material in UK					✔
	pornography				✔	
	promotion of any kind of discrimination					✔
	promotion of racial or religious hatred					✔
	threatening behaviour, including promotion of physical violence or mental harm				✔	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✔	

Using school systems to run a private business				✔	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school				✔	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				✔	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				✔	
Creating or propagating computer viruses or other harmful files				✔	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				✔	
On-line gaming (educational)		✔			
On-line gaming (non educational)		✔			
On-line gambling				✔	
On-line shopping / commerce – Office staff for school based resources			✔		
File sharing (using approved methods)		✔			
Use of social networking sites (At school)				✔	
Use of video broadcasting e.g. YouTube (for educational purposes)	✔				

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity e.g.

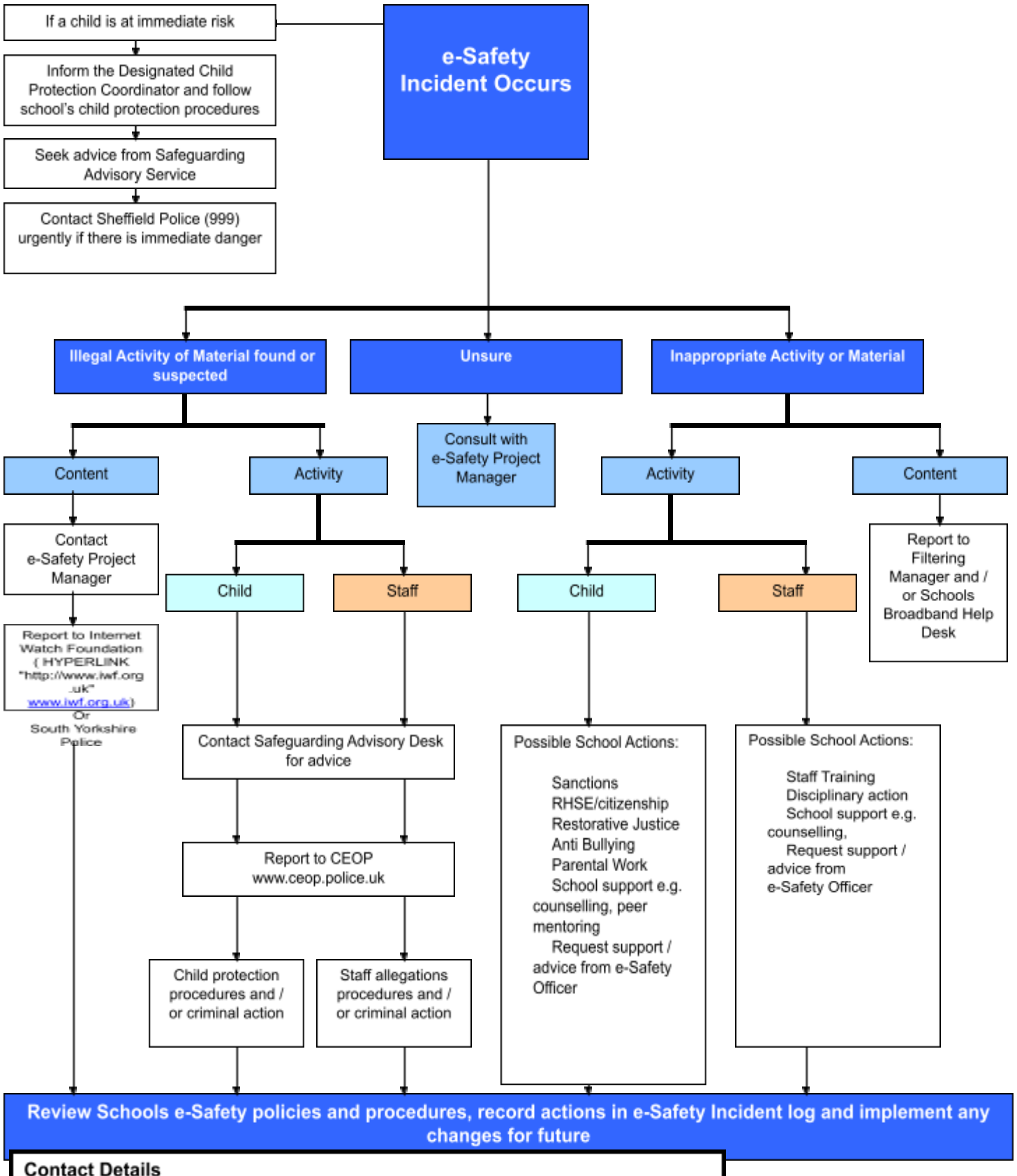
- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The SSCB flow chart should be consulted and actions followed in line with the flow chart.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

Response to an Incident of Concern



Contact Details