Stradbroke Primary E-Safeguarding Policy

Written By	**Written Date**	**Review Date**	**Approved by**
Sue Shelley Abby King	Sep 2020	Sep 2021	Governing body

Policy Introduction

This e-Safeguarding Policy should be read in conjunction with all other school policies. The role of digital technologies in teaching and learning at Stradbroke Primary School provides many benefits and opportunities for every child. However, we also recognise the need to manage potential risks and are committed to safeguarding children whilst promoting the positive use of ever changing technologies. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils and it is an integral part of computing education for pupils to be taught how to use it responsibly. At school, we therefore aim to help young people, their parents/carers and all staff to be responsible users and stay safe while using the internet and other communication technologies for educational and personal use.

This e-Safeguarding Policy considers the use of both the fixed and mobile internet, PCs, laptops, webcams, iPads, digital video equipment, mobile phones, smart phones, personal digital assistants, portable media players and gaming devices. It will be revised to incorporate new and emerging technologies. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Our e-Safeguarding Policy is to be used in conjunction with the school's Acceptable Use Policy and Data Protection Policy, building upon government guidance, to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole. It has been agreed by the senior management team and approved by governors. The school has appointed an e-Safeguarding team, two e-safeguarding co-ordinators Sue Shelley and Kath Cockayne and a safeguarding governor. This e-Safeguarding Policy and its implementation will be reviewed annually to ensure that we are reviewing and updating our school's practice to manage and reduce the risks which new technologies can bring.

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 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 applies to incidents of cyber-bullying, or other e-Safeguarding incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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.

Development, Monitoring and Review of this Policy

This policy has been developed by the e-Safeguarding team:

- School e-Safety Coordinators- Sue Shelley and Kath Cockayne
- Headteacher/Senior Leadership Team- John Sitch and Stephen Nash
- E-Safeguarding Governor- Natalie Swallow

Consultation with the whole school community (teachers, support staff, ICT technician and governors) has taken place through the following:

- Staff meetings
- School Council
- INSET Day
- Governors meeting/sub-committee meeting
- Parents evening
- School website/newsletters

Schedule for Development, Monitoring and Review.

Because of the regular updates of the policy there may be many versions created. Each version will be stored for audit purposes.

Title	**E-Safeguarding Policy**
Version	1.5
Date	*10/9/20*
Author	*Sue Shelley and Abby King*
This E-Safeguarding policy was approved by the Governing Body on*:*	
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:	In the Headteacher's report.
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:	*September 2021*
Should serious E-Safeguarding incidents take place, the following external persons / agencies should be informed:	*Sheffield LA E-Safety Project Manager Julia Codman, LA Safeguarding Officer, Police Commissioner's Office.*
Should serious E-Safeguarding incidents take place, the following internal persons should be informed:	*John Sitch (Headteacher & Safeguarding Lead), Sue Shelley (Safeguarding Lead and E-Safeguarding Co-ordinator) Kath Cockayne (Designated Safeguarding Deputy).*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Internal monitoring data for network activity (Smoothwall monitored by safeguarding lead)
- Surveys/questionnaires of pupils, parents/carers and staff

All staff and members of the school community must be informed of any relevant amendments to the policy.

Communication of the Policy

Stradbroke'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. The e-Safeguarding Policy will be provided to all members of staff. All amendments will be published and awareness sessions will be held for all members of the school community.

As part of the curriculum, pupils will be made aware of the Acceptable User Policy for the Internet. These guidelines for acceptable use will be clearly on display in all classrooms in a child friendly format and pupils will sign to agree to them. E-Safeguarding updates will be integrated within the computing curricula and pupils' responsibilities regarding the school e-Safeguarding Policy will be continually reviewed.

All pupils will be given clear objectives when using the internet and safeguarding posters will be prominently displayed around the school. Where internet activities are part of the curriculum, they will be planned so that they enrich and extend the learning activities. Staff will guide pupils through online activities that will support the learning outcomes planned for the age and maturity of the pupils. Internet use will be supervised to ensure it will be age appropriate. We endeavour to embed e-Safeguarding messages across the curriculum whenever the internet or related technologies are used.

Roles and Responsibilities

The school will ensure that all members of the school community are aware of the e-Safeguarding Policy and the implications for the individual. E-Safety depends on staff, governors, parents and, where appropriate, the pupils themselves taking responsibility for the use of the internet and other communication technologies.

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 Co-ordinators.
- The Headteacher and Senior Leadership Team are responsible for ensuring that the e-Safeguarding Co-ordinator 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 Headteacher will receive monitoring reports from the e-Safeguarding Co-ordinator.
- 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 Committee

- 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's Acceptable Use Policy is 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 Co-ordinates

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 Eucation 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 e-Safeguarding incidents are recorded and logged using CPOMS.

Responsibilities of the Teaching and Support Staff

- To read, understand and help promote the school's e-Safeguarding policies and guidance.
- To read, understand and adhere to the school's Acceptable Use Policy.
- To report any suspected misuse or problem to the e-Safeguarding Co-ordinator and record all issues on CPOMS.
- 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.
- 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.
- To supervise and guide pupils carefully when engaged in learning activities involving technology.
- To ensure that pupils are fully aware of research skills and are fully aware of 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 (CPOMS).
- To maintain a professional level of conduct in personal use of technology at all times.
- 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.
- To read, understand and adhere to the school's Acceptable Use Policy.
- To report any e-Safeguarding related issues that come to your attention to the e-Safeguarding Co-ordinator.
- 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 e-mail, 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.
- 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 practices 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 on the taking and use of mobile phones.
- 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. This includes all forms of online gaming and use of home gaming devices.
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home. This includes all forms of online gaming and use of home gaming devices.
- 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. (see copy of home school agreement).

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-Safeguarding Governor includes:

- Regular meetings with the e-Safeguarding Co-ordinator
- Regular monitoring of e-Safeguarding incident logs
- Reporting in Governors meetings

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

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 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:

- We will provide a series of specific e-Safeguarding-related lessons in every year group/specific year groups as part of the Computing curriculum and embedded within other lessons where appropriate.
- We will celebrate and promote e-Safeguarding through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year or through designated an e-Safety Week.
- 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 our child friendly Acceptable Use Policy which every pupil will sign and have displayed in their classroom.
- 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-Safeguarding 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.
- An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff receives 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 / team meetings / INSET days.
- The e-Safeguarding Co-ordinator 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

- parents' evenings
- newsletters
- letters
- website/VLE
- information about national/local e-safety campaigns/literature

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 and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying 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.
- 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.

- 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.
- 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 social media sites, particularly in association with photographs, without parental consent.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or social media accounts.
- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

Managing ICT systems and access

The school has a managed ICT service provided by an outside contractor Viglen, we are responsible for ensuring that the managed service provider carries out all the e-safety measures.

The school has a variety of hardware, software, infrastructure and connectivity in providing ICT access to the school community. We ensure that access to any equipment and the use of the internet is as safe and secure as is reasonably possible and that all risks relating to any type of ICT equipment usage have been identified and managed. The school assesses the risk involved in using all types of equipment within school termly, so that appropriate measures can be put in place to reduce risks to an acceptable level.

The school is also aware of any policies or procedures which are inherited as part of our responsibilities to the local authority or Local Safeguarding Children Board. All internal policies and procedures have the appropriate level of visibility within the school. All staff and pupils have completed the appropriate awareness training and where appropriate signed to confirm that they understand what is deemed to be acceptable for using equipment and staying safe. This is done by:

- The school is 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 has agreed which users should and should not have internet access and the appropriate level of access and supervision they should receive.
- Members of staff access the internet using an individual id and password, which are kept secure. They ensure that they log out after each session and do 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

'Pupils in the schools that had 'managed' systems had better knowledge and understanding of how to stay safe than those in schools with 'locked down' systems. Pupils were more vulnerable overall when schools used 'locked down' systems because they were not given enough opportunities to learn how to assess and manage risk for themselves.'

- The school uses a filtered internet service. The filtering system is provided by Smoothwall.
- 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 has 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 Coordinator. 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, Child Exploitation and Online Protection Command (CEOP) or the Internet Watch Foundation (IWF).
- Through the Smoothwall safeguarding system the school will regularly review the filtering product for its effectiveness.
- The school filtering system will block all sites on the IWF 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. Staff need to consult with phase leaders with regards to any sites to be unblocked.
- 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.
- The head teacher and safeguarding lead will receive regular reports from Smoothwall with regards to possible inappropriate sites. They will respond to any issues when required.

Passwords

Passwords are an important aspect of computer security. They are the front line of authentication for the protection of user accounts and their associated access to ICT equipment and resources. A poorly-chosen password may result in the compromise of a pupil's work, sensitive information regarding pupils or staff being lost or stolen or a school's or local authority's network being infected or attacked.

Stradbroke has a responsibility to ensure that all elements of the school infrastructure and network equipment are as safe and secure as possible. All staff and pupil access to school-owned equipment and information assets are controlled through the use of appropriate username and password complexity policies.

- A secure and robust username and password convention exists for all system access (e-mail, network access, school management information system).
- Pupils will have a generic 'pupil' logon 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, e.g.

- 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 Data Protection Policy.
- The school maintains a log of all accesses by users and of their activities while using the system.
- Passwords must contain a minimum of eight characters and be difficult to guess.
- Users should create different passwords for different accounts and applications.
- Users should be advised to 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 are recorded in a hardware inventory.
- Details of all school-owned software are 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 most recent amended version of The Waste Electrical and Electronic Equipment Regulations 2013.

Data Protection

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This applies to all personal data, regardless of whether it is in paper or electronic format and our approach is outlined fully in the school's Data Protection Policy.

Communication Technologies

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

- The official school e-mail service may be regarded as safe and secure and is monitored. Staff and 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 e-mail that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such e-mail.
- Any digital communication between staff and students / 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 all 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					X
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					X
	adult material that potentially breaches the Obscene Publications Act in the UK					X
	criminally racist material in UK					X
	pornography				X	
	promotion of any kind of discrimination				X	
	promotion of racial or religious hatred				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Smoothwall and / or the school					x	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					x	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
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					X	
On-line gaming (educational)				X		
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce					X	
File sharing					X	
Use of social networking sites				X		
Use of video broadcasting e.g. Youtube				X		

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

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 as follows:

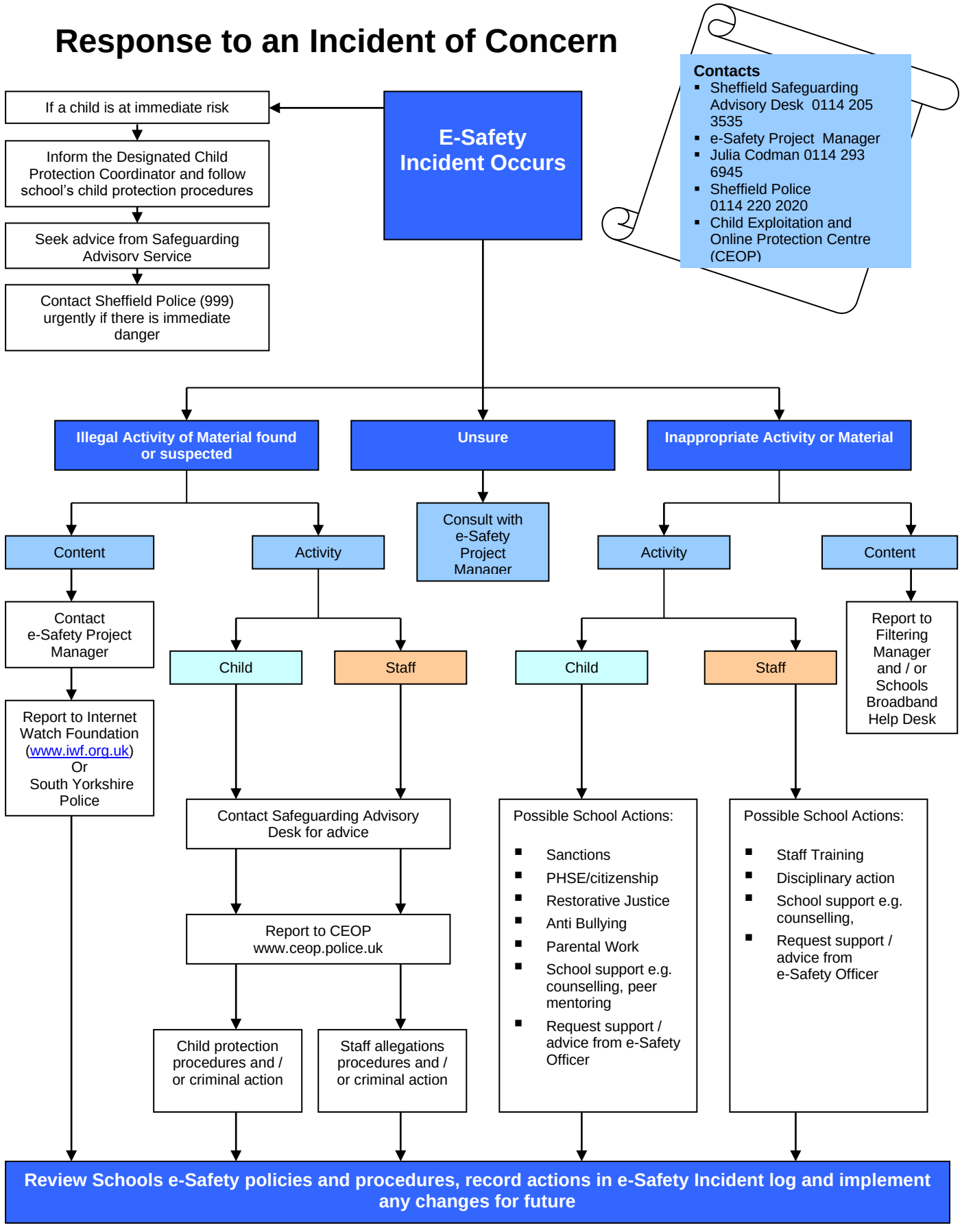
Pupils Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	X								
Unauthorised use of mobile phone / digital camera / other handheld device	X								
Unauthorised use of social networking / instant messaging / personal email	X								
Unauthorised downloading or uploading of files	X								
Allowing others to access school network by sharing username and passwords	X								
Attempting to access or accessing the school network, using another student's / pupil's account	X								
Attempting to access or accessing the school network, using the account of a member of staff	X								
Corrupting or destroying the data of other users	X	X							
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X				X			
Continued infringements of the above, following previous warnings or sanctions	X	X	X			X			
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X			X			
Using proxy sites or other means to subvert the school's filtering system	X	X	X			X			
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X			X			
Deliberately accessing or trying to access offensive or pornographic material	X	X	X			X			
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X			X			

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	X	X						
Unauthorised downloading or uploading of files	X	X						
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X						
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X						
Deliberate actions to breach data protection or network security rules	X	X						
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X						
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X						
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X						
Actions which could compromise the staff member's professional standing	X	X						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X						
Using proxy sites or other means to subvert the school's filtering system	X	X						
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X						
Deliberately accessing or trying to access offensive or pornographic material	X	X						
Breaching copyright or licensing regulations	X	X						
Continued infringements of the above, following previous warnings or sanctions	X	X						

Response to an Incident of Concern



Contact Details

Schools Designated Child Protection Officer: Sue Shelley
School e-Safety Coordinator: Sue Shelley and Kath Cockayne
Safeguarding Children Board e-Safety Manager: Sue Shelley