Rainbow Forge
Primary School

Learning Together, Succeeding Forever

Rainbow Forge Primary School

E-Safety Policy

Policy Introduction

The use of digital technology within our school curriculum is paramount in our rapidly changing and expanding technological world. It is important that children and staff remain up to date with new and emerging technology. Digital technology is used to support all areas of the curriculum, and skills are also taught explicitly through ICT lessons.

Whilst we embrace the exciting opportunities which digital technology presents, we also realize the potential risks involved. The school is committed to ensuring that children are safe when using all types of technology in school, but also that they learn how to keep themselves safe in the wider world.

The e-safeguarding policy that follows explains how we intend to keep children safe, while also addressing wider educational issues in order to help young people, their parents / carers and all staff to be responsible users and stay safe while using the internet and other communications technologies for educational and personal use.

Scope of the Policy

- This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, work placement students, visitors, 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 students / 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 / Review of this Policy

This policy has been developed by a working group made up of:

- School E-Safety Coordinator
- Headteacher
- Inclusion Leader
- Governors (environment group)

Consultation with the whole school community has taken place through the following:

- Staff meetings
- School Council
- Training session lead by Julia Codman
- Governors environment group meeting
- Parent forum
- School website / newsletters

Schedule for Development / Monitoring / Review

Title	**E-Safeguarding Policy**
Version	1.0
Date	*26/11/2014*
Author	*E-safety Co-ordinator/Headteacher*
This e-safeguarding policy was approved by the Governing Body on*:*	
Monitoring will take place at regular intervals (at least annually):	*Every 2 years*
The Governing Body will receive a report on the implementation of the policy including anonymous details of any e-safeguarding incidents at regular intervals:	*Every 2 years*
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:	*November 2016*
Should serious e-safeguarding incidents take place, the following external persons / agencies should be informed:	*LA ICT Manager* *Julia Codman* *Safeguarding Children Advisory Service* *0114 2053535*

- The school will monitor the impact of the policy using:
- Logs of reported incidents
- Internal monitoring data for network activity (YHGfL data - termly)
- Surveys / questionnaires of
  - students / pupils (including Every Child Matters Survey)
  - parents / carers
  - staff

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

Communication of the Policy

- The schools 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 eSafeguarding policy and the use of any new technology within school.

- The eSafeguarding policy will be provided to and discussed with all members of staff formally.

- All amendments will be published and awareness sessions will be held for all members of the school community.

- Any amendments to the acceptable use policy will be discussed by the School Council to ensure the language and vocabulary is appropriate and understandable for the policy's intended audience.

- An eSafeguarding or eSafety module will be included in the PSHE, Citizenship and/or ICT curricula covering and detailing amendments to the eSafeguarding policy.

- eSafeguarding or eSafety training will be part of the transition programme across the Key Stages.

- Pertinent points from the school eSafeguarding policy will be reinforced across the curriculum and across all subject areas when using ICT equipment within school.

- The key messages contained within the eSafeguarding policy will be reflected and consistent within all acceptable use policies in place within school.

- We endeavour to embed eSafeguarding messages across the curriculum whenever the internet or related technologies are used

- The eSafeguarding policy will be introduced to the pupils at the start of each school year

- Safeguarding posters will be prominently displayed around the school

Roles and Responsibilities

We believe that eSafeguarding 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 Co-ordinator.
- The headteacher and senior leadership team are responsible for ensuring that the eSafeguarding Coordinator and other relevant staff receive suitable training to enable them to carry out their eSafeguarding 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 eSafeguarding monitoring role. This provision provides a safety net and also supports those colleagues who take on important monitoring roles.
- The senior leadership team will receive monitoring reports from the eSafeguarding Coordinator.
- The headteacher and senior leadership team should ensure that they are aware of procedures to be followed in the event of a serious eSafeguarding incident.
- The headteacher and senior leadership team should receive update reports from the incident management team.

Responsibilities of the eSafeguarding group

- To ensure that the school eSafeguarding policy is current and pertinent.
- To ensure that the school eSafeguarding 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 Coordinator

- To promote an awareness and commitment to eSafeguarding throughout the school.
- To be the first point of contact in school on all eSafeguarding matters and liase with Childre Protection Liason Officer about safeguarding incidents.
- To take day-to-day responsibility for eSafeguarding within school and to have a leading role in establishing and reviewing the school eSafeguarding policies and procedures.
- To lead the school eSafeguarding group or committee.
- To have regular contact with other eSafeguarding committees, e.g. Safeguarding Children Board
- To communicate regularly with school technical staff.
- To communicate regularly with the designated eSafeguarding governor (David Hoar).
- To communicate regularly with the senior leadership team.
- To create and maintain eSafeguarding policies and procedures.
- To develop an understanding of current eSafeguarding issues, guidance and appropriate legislation.

- To ensure that all members of staff receive an appropriate level of training in eSafeguarding issues.
- To ensure that eSafeguarding education is embedded across the curriculum.
- To ensure that eSafeguarding is promoted to parents and carers.
- To liaise with the local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate or to liase with CPLO.
- To monitor and report on eSafeguarding issues to the eSafeguarding 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 eSafeguarding incident.
- To ensure that an eSafeguarding incident log is kept up to date (digitally).

Responsibilities of the Teaching and Support Staff

- To read, understand and help promote the school's eSafeguarding policies and guidance.
- To read, understand and adhere to the school staff Acceptable Use Policy.
- To report any suspected misuse or problem to the eSafeguarding coordinator.
- To develop and maintain an awareness of current eSafeguarding 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 eSafeguarding 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 eSafeguarding 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.
- 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 eSafeguarding policies and guidance.
- To read, understand and adhere to the school staff Acceptable Use Policy.
- To report any eSafeguarding related issues that come to your attention to the eSafeguarding coordinator.
- To develop and maintain an awareness of current eSafeguarding 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 eg 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 Students / pupils

- To read, understand and adhere to the school pupil Acceptable Use Policy.
- To help and support the school in the creation of eSafeguarding 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.
- 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 eSafeguarding issues with family and friends in an open and honest way.

Responsibilities of Parents / Carers

- To help and support the school in promoting eSafeguarding.
- 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 eSafeguarding 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.

To sign a home-school agreement containing the following statements:

- *We will support the school approach to online safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community*
- *We will support the school's stance on the use of ICT and ICT equipment*
- *Images taken of pupils at school events will be for personal use only and not uploaded or shared via the internet*
- *Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites*

- *Parents and carers are asked to read through and sign acceptable use agreements on behalf of their children on admission to school and then annually thereafter.*
- *Parents and carers are required to give written consent for the use of any images of their children within school or school website/blog. Ocasionally, additional consent may be asked for when involving outside groups in the form of a letter or text message (usually provided by the outside group)*

Responsibilities of the Governing Body

- To read, understand, contribute to and help promote the school's eSafeguarding 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 eSafeguarding group in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in eSafeguarding activities.
- To ensure appropriate funding and resources are available for the school to implement its eSafeguarding strategy.

The role of the E-Safety Governor includes:

- regular liason with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- reporting to Governors meeting

Responsibilities of Other Community/ External Users

- The school will liaise with local organisations to establish a common approach to eSafeguarding 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 staff, students or volunteers 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 other 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

Students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating students / pupils to take a responsible approach. The education of students / 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:

- We will provide a series of specific eSafeguarding-related lessons as part of the ICT curriculum/PHSE.
- We will celebrate and promote eSafeguarding through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant eSafeguarding 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 end-user Acceptable Use Policy which every pupil will sign/will be displayed throughout the school.(including ICT suite and classrooms)
- 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:

- 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 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 Coordinator 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

- Parent forum
- Newsletters
- Letters
- Website
- 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 students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students / 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 eg 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. Where staff use their personal devices, files should be transferred to a password protected staff laptop as soon as possible and the images deleted.

- 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. (permission will be obtained annually)

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

Managing ICT systems and access

Each school will have different arrangements of hardware, software, infrastructure and connectivity in providing ICT access to the school community. The key here is that the school will need to 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 in accordance with the school's senior leadership team's stance and its approach to risk. It is very important that all schools assess the risk involved in using all types of equipment within school, so that appropriate measures can be put in place to reduce risks to an acceptable level.

Schools also need to be aware of any policies or procedures which are inherited as part of their responsibilities to their local authority or Local Safeguarding Children Board. All internal policies and procedures should have the appropriate level of visibility within school in an attempt to ensure that they are implemented accordingly. All staff and pupils should 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.

- 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 on the appropriate level of access to the internet and supervision users should receive.
- Members of staff will access staff laptops 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 computers through their ID and password. They will abide by the school AUP at all times.

Filtering internet access

As all schools will be aware, the internet is a valuable tool for teaching and learning. Unfortunately, not all content that is available on the internet is suitable for schools, so provision has to be made to ensure that a suitable, fit-for-purpose internet filtering solution is deployed. As with any aspect of education, decisions and guidance from OFSTED very much influence what schools need and want. The OFSTED report, 'Safe use of new technologies' (February 2010) had, as one of its key findings,

'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 YHGfL
- 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 documented using the appropriate proforma, then emailed to the E-Safeguarding co-ordinator.
- If users discover a website with potentially illegal content, this should be reported immediately to the eSafeguarding 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).
- 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 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 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 personal data 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 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 the school 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.

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 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 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 device must offer approved virus and malware checking software
    - 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

If you are transmitting sensitive information or personal data e.g. by email or fax it must be transferred by a secure method so it is protected from unauthorised access.

Email

If sensitive data is sent via email, it is encrypted prior to being sent. **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 fax will be transferred using a secure method.

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	x				X(office)			
Use of mobile phones in lessons		x						x
Use of mobile phones in social time	x							x
Taking photos on mobile phones or other camera devices	x						x	
Use of hand held devices eg PDAs, PSPs	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				x				X
Use of instant messaging				x			x	
Use of social networking sites		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 students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg 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 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 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 SWGfL 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 (eg 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	X		
File sharing		X	X		
Use of social networking sites		x	x		
Use of video broadcasting eg 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

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 as follows:

Students / Pupils

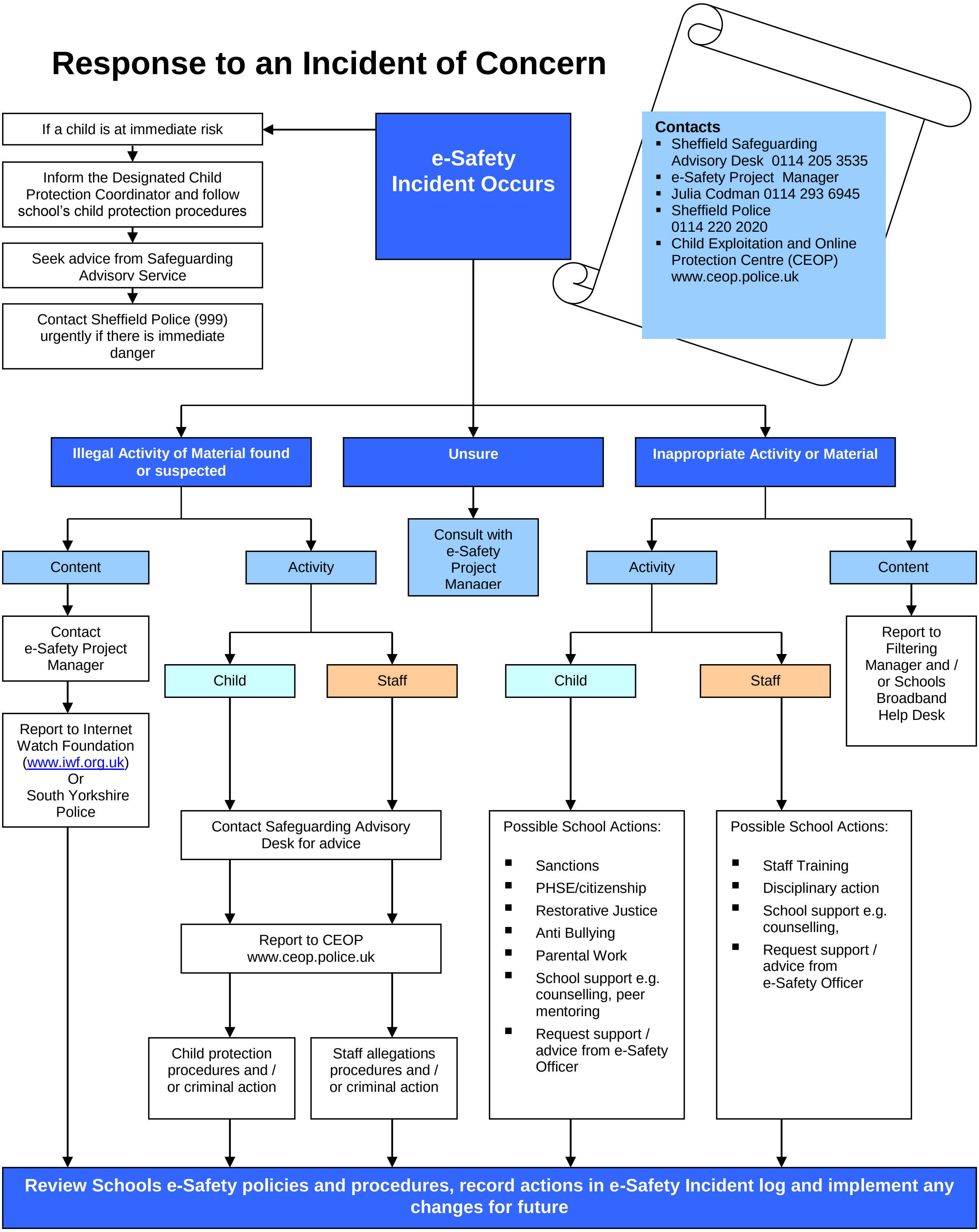
Actions / Sanctions

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		x			x		x	
Unauthorised use of mobile phone / digital camera / other handheld device	x		x			x		x	
Unauthorised use of social networking / instant messaging / personal email	x		x			X		x	
Unauthorised downloading or uploading of files	x		x		x	x		x	
Allowing others to access school network by sharing username and passwords	x		x			x		x	
Attempting to access or accessing the school network, using another student's / pupil's account	x		x		x	x		x	
Attempting to access or accessing the school network, using the account of a member of staff	x		x		x	x		x	
Corrupting or destroying the data of other users	x		x		x	x		X	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	x		x	x	x	x		x	
Continued infringements of the above, following previous warnings or sanctions	x		x	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		x	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	x		x		x	x		x	

Staff Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Headteacher	RRefer 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	x			x
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		x			x	x		
Unauthorised downloading or uploading of files		x			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	X		
Careless use of personal data eg holding or transferring data in an insecure manner		x			X	x		
Deliberate actions to breach data protection or network security rules		x			x	x		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x			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	x		
Deliberately accessing or trying to access offensive or pornographic material		x			X			x
Breaching copyright or licensing regulations		x			x	x		
Continued infringements of the above, following previous warnings or sanctions		x			x			x

Response to an Incident of Concern



e-Safety Incident Occurs

If a child is at immediate risk

Inform the Designated Child Protection Coordinator and follow school's child protection procedures

Seek advice from Safeguarding Advisory Service

Contact Sheffield Police (999) urgently if there is immediate danger

Contacts

- Sheffield Safeguarding Advisory Desk 0114 205 3535
- e-Safety Project Manager
- Julia Codman 0114 293 6945
- Sheffield Police 0114 220 2020
- Child Exploitation and Online Protection Centre (CEOP) www.ceop.police.uk

Illegal Activity of Material found or suspected

Content

Contact e-Safety Project Manager

Report to Internet Watch Foundation (www.iwf.org.uk) Or South Yorkshire Police

Activity

Child

Staff

Contact Safeguarding Advisory Desk for advice

Report to CEOP www.ceop.police.uk

Child protection procedures and / or criminal action

Staff allegations procedures and / or criminal action

Unsure

Consult with e-Safety Project Manager

Inappropriate Activity or Material

Activity

Child

Possible School Actions:

- Sanctions
- PHSE/citizenship
- Restorative Justice
- Anti Bullying
- Parental Work
- School support e.g. counselling, peer mentoring
- Request support / advice from e-Safety Officer

Staff

Possible School Actions:

- Staff Training
- Disciplinary action
- School support e.g. counselling,
- Request support / advice from e-Safety Officer

Content

Report to Filtering Manager and / or Schools Broadband Help Desk

Review Schools e-Safety policies and procedures, record actions in e-Safety Incident log and implement any changes for future

Contact Details

Schools Designated Child Protection Officer:

School e-Safety Coordinator:

Safeguarding Children Board e-Safety Manager: