



# Sheffield Safeguarding Children Board

Primary  
**ECCLESALL**  
School

Online Safety Policy  
2023-24

# Content

Introduction

Creating an E-Safeguarding Policy

Policy Introduction and Scope of the Policy

Development, monitoring and review of the Policy

Schedule for development, monitoring and review

Roles and Responsibilities

Education

Use of digital and video images

Managing ICT Systems and Access

Management of Assets

Data Protection

Communication Technologies

Managing Unsuitable and Inappropriate Activities

Response to an Incident Flowchart

Appendices:

- Student / Pupil Acceptable Use Policy Agreement Template
- Staff and Volunteers Acceptable Use Policy Agreement Template
- Parents / Carers Acceptable Use Policy Agreement Template
- Use of Digital Images and Consent Form
- Mobile Phone Use
- Questions for Schools
- Links to other organisations, documents and resources
- Legislation

# Introduction

This School Online Policy Template is intended to help school leaders produce a suitable policy document and clear Acceptable Use Policies (AUPs) which will outline their schools approach to safe and responsible use of technology.

## Why have an E-Safeguarding Policy?

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safeguarding policy should help to ensure safe and appropriate use by all users.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement. However, the use of these new technologies can put users at risk. The breadth of issues within e-safeguarding is considerable, but they can be categorised into three areas of risk:-

- Content:** being exposed to illegal, inappropriate or harmful material  
**Contact:** being subjected to harmful online interaction with other users  
**Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

Many of these risks reflect situations in the off-line world so it is essential that this e-Safeguarding policy is used in conjunction with other policies (e.g. safeguarding and child protection policies / anti-bullying / behaviour etc.) Creating an E-Safeguarding policy is not an easy task and this document is designed to enable you to begin to create a policy or review and adapt your current policy.

## Creating the Policy

The template suggests policy statements which, in the view of Sheffield Safeguarding Children Board (SSCB), would be essential in any school E-Safeguarding Policy based on good practice and the experience of incidents at schools across the region.

An effective School E-Safeguarding Policy must be tailored to the needs of each school and an important part of the process will be the discussion and consultation which takes place during the writing or review of the policy. This will help ensure that the policy is owned and accepted by the whole school community. It is suggested that consultation in the production of this policy should involve:

- Senior Management Team, Governors, Teaching Staff and Support Staff
- Students / pupils
- Parents
- Community users and any other relevant groups

Because of the range of documents provided, this template document is much longer than the resulting school policy will be. It is intended that the resulting policy should be concise and easily understood, if it is to be effective and adopted by all.

Within this template sections which include information or guidance are shown in **RED**. It is anticipated that schools would remove these sections from their completed policy document.

**Where sections are highlighted in BOLD text, it is viewed that these would be an essential part of a school e-safeguarding policy.**

*Where sections in the template are written in italics it is anticipated that schools would wish to consider whether or not to include that section or statement in their completed policy.*



# Ecclesall Primary School

## Online Safety Policy

# Policy Introduction

Technology is an important and essential part of the learning experience at Ecclesall Primary School. We are committed to ensuring that our children leave with the skills and knowledge that will help them to thrive in our digital age. We have laptops in every year group and ipads are planned to be part of everyday research and use. The teachers use the internet daily with the children. It is therefore also vital that we teach children how to use this valuable resource safely. This policy will appreciate that all children have access to smart phones, ipads and computers at home and within school. It promotes the use of these technologies whilst committing to keeping our children aware of and safe from the potential risks.

We will demonstrate that we have provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. The e-safeguarding policy that follows explains how we intend to do this, 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

- School E-Safety Coordinator
- Headteacher / Senior Leadership Team
- ICT Technical staff
- Governors

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

- Staff meetings
- School Council
- Governors sub- committee meeting
- School website

# Schedule for Development / Monitoring / Review

Title	<b>E-Safeguarding Policy</b>
Version	1.0
Date	6/11/13, Updated September 2014.
Author	E-safety Co-ordinator/Team
	Executive Head – Emma Hardy E Safety Leader – Stephen Young
This e-safeguarding policy was approved by the Governing Body on:	19/11/13
Monitoring will take place at regular intervals (at least annually):	Termly
The Governing Body will receive a report on the implementation of the policy including anonymous details of any e-safeguarding incidents at regular intervals:	Termly – Head teacher 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:	November 2014
Should serious e-safeguarding incidents take place, the following external persons / agencies should be informed:	LA Safeguarding Officer - Julia Codman 0114 2736945. Police Office – 0114 202020.

- The school will monitor the impact of the policy using:
  - Logs of reported incidents
  - Internal monitoring data for network activity
  - 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

## Key steps

- Decide how your eSafeguarding policy or any amendments will be published.
- Detail this process within a short paragraph in this section.
- Consider the issues in the following statements, and discuss how you will address these within your school. Then adapt or replace the statements to reflect your approach. Add any additional statements you need.

## Possible statements

- Ecclesall Primary School'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 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 during a Professional Development Meeting.
- All amendments will be published and alerts sent out on the school website for parents and during the briefing sessions for staff.
- Any amendments will be discussed by the School Council to ensure the language and vocabulary is appropriate and understandable for the policy's intended audience.
- An eSafeguarding or eSafety module will be included in the PSHE, Citizenship and/or ICT curricula covering and detailing amendments to the eSafeguarding policy.
- 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 Committee – Head, Deputy and Phase Leaders.

- 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.
- 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.
- 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.
- 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.

### 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 – Viglen IT Consultancy

- 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 be issued with the home/school agreements in the Autumn term.*
- 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.

( From 2014) To read and adhere to 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 unless appropriate security settings are enabled and set to maximum*
- *Parents and carers are required to give written consent for the use of any images of their children in a variety of different circumstances.*

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

## Responsibilities of Other Community/ External Users

*Community Users who access school ICT systems / website / VLE as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.*

- 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 external organisations will sign an Acceptable Use Policy prior to using any equipment or the internet within school.
- The school will provide an Acceptable Use Policy for any guest who needs to access the school computer system or internet on school grounds.
- The school will ensure that appropriate levels of supervision exist when external organisations make use of the internet and ICT equipment within school.



# Education

## Pupils

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

- *We will provide a series of specific eSafeguarding-related lessons in every year group/specific year groups as part of the ICT curriculum / PSHE curriculum / other lessons. 2014 Curriculum.*
- 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 will be displayed throughout the school and **will be displayed when a pupil logs on to the school network.**
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- All pupils will be taught in an age-appropriate way about copyright in relation to online resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the internet.
- Pupils will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button

## All Staff (including Governors)

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

- A planned programme of formal e-safety training will be made available to staff.
- 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 / team meetings / INSET days.
- The E-Safety Coordinator with the headteacher 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

- Annual Parent information evening
- 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:

## Possible statements

- 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, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- **Pupils must not take, use, share, publish or distribute images of others without their permission.**
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before pupils are published on the school website. Parents are asked to send a negative response at the beginning of the year and this is kept on file.
- Pupil's work can only be published with the permission of the pupil and parents or carers.
- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

# Managing ICT systems and access

## Possible statements

- 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. ( Locked in library cupboard)
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- The school will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive. At Key Stage 2, pupils will have an individual user account with an appropriate password which will be kept secure, in line with the pupil Acceptable Use Policy. They will ensure they log out after each session.
- Members of staff will access the internet using an individual id and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their id and password. They will abide by the school AUP at all times.

# Filtering internet access

***'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.'***

## Possible statements

- The school uses a filtered internet service. The filtering system is provided by Yorkshire Humber Grid for Learning.
- The school's internet provision will include filtering appropriate to the age and maturity of pupils.
- The school will always be proactive regarding the nature of content which can be viewed through the school's internet provision.
- The school will have a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading 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 eSafeguarding Coordinator. **All incidents should be documented.**

- 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

## Key steps

- Your school **Senior Information Risk Officer** should go through the process of assessing the risk of using different technologies in use within school.
- Once this process has been completed, appropriate controls should be highlighted and recommendations made regarding what access should be protected through the use of usernames and passwords.
- Once this has been established, suitable technical controls and authentication mechanisms should then be implemented.
- Consider the issues in the following statements, and discuss how you will address these within your school. Then adapt or replace the statements to reflect your approach.

## Possible statements

- A secure and robust username and password convention exists for all system access. (email, network access, school management information system).
- Pupils at Key Stage 2 have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- 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 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 a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. [Further information can be found on the Environment Agency website.](#)

# Data Protection

## Personal Data

### Senior Information Risk Owner (SIRO)

The Headteacher is also The Senior Information Risk Owner and is familiar with information risks and the organisation's response. They have the following responsibilities

- They own the information risk policy and risk assessment
- They appoint the information asset owners (IAOs)
- They act as an advocate for information risk management

**The Office of Public Sector Information has produced a publication 'Managing Information Risk' to support SIROs in their role.**

### Information Asset Owner (IAO)

The Business Manager is the IAO for each asset or group of assets within school. The role of an IAO is to understand

- What information is held, and for what purposes
- How information will be amended or added to over time
- Who has access to the data and why
- How information is retained and disposed of

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 Ecclesall Primary School we will:

- 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

We transfer data using the SIMs LA Outbox. This is a secure method and is protected from unauthorised access.

## Email

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

**WE 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

- The Fax machine is situated within controlled areas of the school.
- All sensitive information or personal data sent by email or fax will be transferred using a secure method.
- personal or sensitive information must be within the email itself as the information may be insecure. This can be done by creating a document (e.g. Word document) and then encrypting the document and sending it as an attachment with the email.



# Communication Technologies

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

Communication Technologies	Staff & other adults				Students / Pupils			
	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	Y						Y	
Use of mobile phones in lessons				Y				N
Use of mobile phones in social time					Y			N
Taking photos on mobile phones or other camera devices					Y			N
Use of hand held devices eg PDAs, PSPs		Y						N
Use of personal email addresses in school, or on school network				N				N
Use of school email for personal emails				N				N
Use of chat rooms / facilities				N				N
Use of instant messaging		Y						N
Use of social networking sites				Y				N
Use of blogs		Y					Y	

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

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (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 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
<b>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:</b>	child sexual abuse images					❖
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					❖
	adult material that potentially breaches the Obscene Publications Act in the UK					❖
	criminally racist material in UK					❖
	pornography				❖	
	promotion of any kind of discrimination				❖	
	promotion of racial or religious hatred				❖	
	threatening behaviour, including promotion of physical violence or mental harm				❖	
any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				❖		
<b>Using school systems to run a private business</b>					❖	
<b>Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school</b>					❖	
<b>Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions</b>					❖	
<b>Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)</b>					❖	
<b>Creating or propagating computer viruses or other harmful files</b>					❖	
<b>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</b>					❖	
<b>On-line gaming (educational)</b>					❖	
<b>On-line gaming (non educational)</b>					❖	

On-line gambling				❖	
On-line shopping / commerce		❖			
File sharing				❖	
Use of social networking sites		❖			
Use of video broadcasting eg Youtube		❖			

## 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:

## Pupils

## Actions / Sanctions

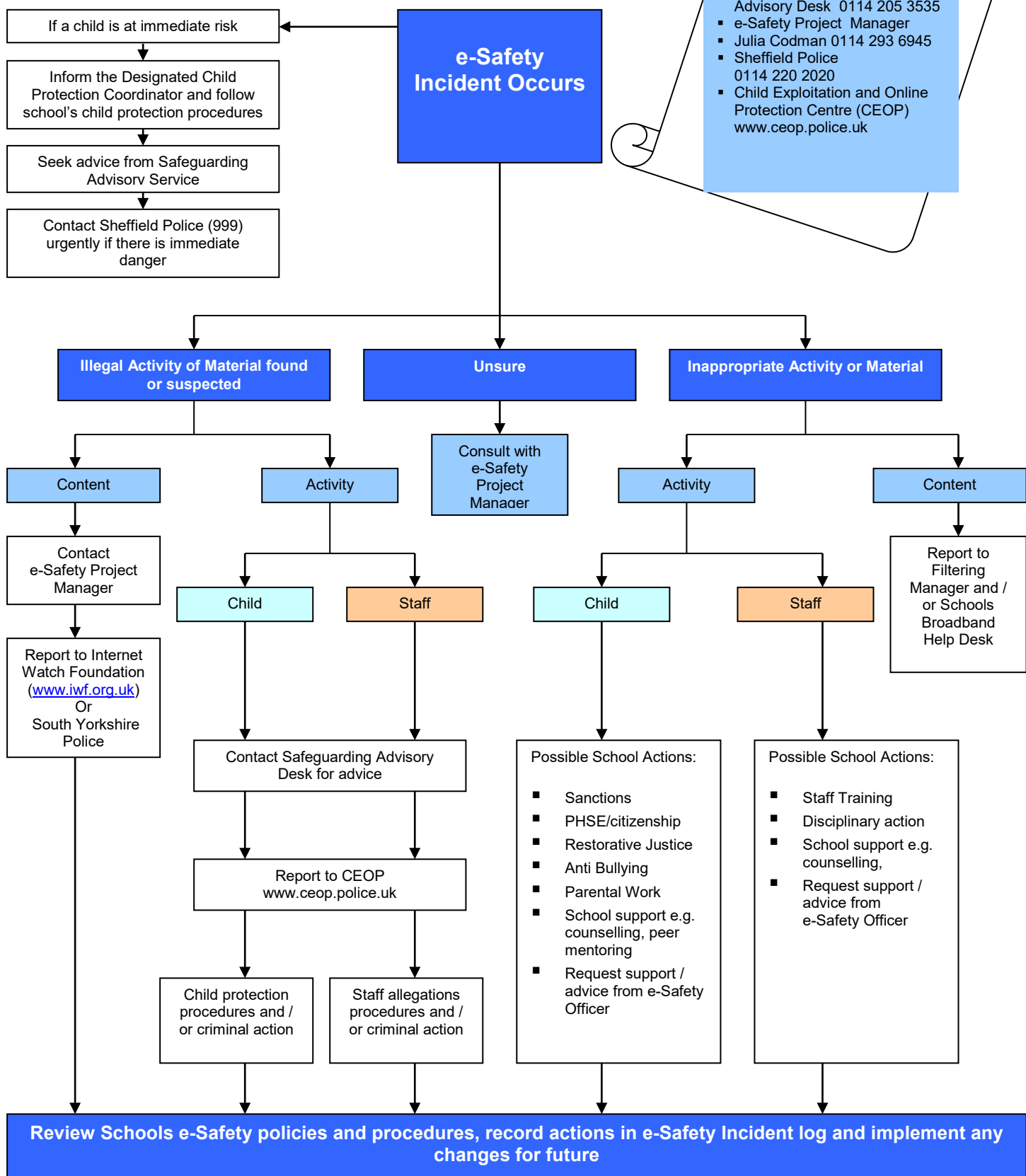
Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention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

## 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
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</b>		❖	❖	❖				
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		❖				❖		❖
Unauthorised downloading or uploading of files		❖				❖		
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						❖		
Careless use of personal data eg holding or transferring data in an insecure manner		❖				❖		
Deliberate actions to breach data protection or network security rules		❖				❖		❖
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		❖	❖	❖			❖	❖
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		❖	❖	❖				❖
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		❖				❖		❖
Actions which could compromise the staff member's professional standing		❖				❖		❖
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		❖	❖					❖
Using proxy sites or other means to subvert the school's filtering system		❖				❖		❖
Accidentally accessing offensive or pornographic material and failing to report the incident		❖						
Deliberately accessing or trying to access offensive or pornographic material		❖	❖	❖			❖	❖
Breaching copyright or licensing regulations		❖				❖		
Continued infringements of the above, following previous warnings or sanctions		❖	❖					❖

# Response to an Incident of Concern



**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

**Contact Details**

Schools Designated Child Protection Officer: Emma Hardy	2361992
School e-Safety Coordinator: Stephen Young	2361992
Safeguarding Children Board e-Safety Manager: Flora Bandele	2053535

# Appendices

- Student / Pupil Acceptable Usage Policy template
- Staff and Volunteers Acceptable Usage Policy template
- Parents / Carers Acceptable Usage Policy Agreement template
- Use of Digital Images and sample Consent Form
- Mobile Phone Use
- Questions for Schools to consider
- Links to other organisations, documents and resources
- Legislation

# Pupil Acceptable Use Policy Agreement Template

## School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

**This Acceptable Use Policy is intended to ensure:**

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that *students / pupils* will have good access to ICT to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users.

## Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

**For my own personal safety:**

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will not share my username and password with anyone or try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

**I understand that everyone has equal rights to use technology to support our education:**

- I understand that the school ICT systems are for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing.  
I will only use youtube if I have permission to do so,

**I will act as I expect others to act toward me:**

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.



- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

**I understand that the school has a responsibility to keep the technology secure and safe:**

- I understand that I do not use my own devices in school.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will only use chat and social networking sites with permission and at the times that are allowed and supervised.

**When using the internet for research for my school work, I understand that:**

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I find is accurate, as I understand that the work of others may not be correct.

**I understand that I am responsible for my actions, both in and out of school:**

- I understand that the school could take action against me if I am involved in incidents or inappropriate behaviour that are included in this agreement, when I am out of school as well as in school. Examples of this is cyberbullying, sending/receiving inappropriate images and misuse of personal information.
- I understand that if I do not follow this Acceptable Use Policy Agreement, it will lead to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

**Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.**

# Student / Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Policy (AUP), which it is attached. Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) eg mobile phones, cameras etc
- I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school e.g. through social networks, mobile phones, accessing school email, Learning Platform, website etc.

Name of Student / Pupil

Group / Class

Signed

Date

# Acceptable Use Policy for Young Children (eg for those aged 8 or younger)

## This is how we stay safe when we use computers:

I will ask *a teacher / an adult* if I want to use the computer

I will only use activities that *the teacher /an adult* has told or allowed me to use.

I will take care of the computer and other equipment

I will ask for help from *the teacher / an adult* if I am not sure what to do or if I think I have done something wrong.

I will tell *the teacher / an adult* if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

## Think before you click

S



I will only use the Internet and email with an adult

A



I will only click on icons and links when I know they are safe

F



I will only send friendly and polite messages

E



If I see something I don't like on a screen, I will always tell an adult

My Name:

My Signature:



# Staff Acceptable Use Policy Template 2012

## Guidance for Use

Senior Leadership Teams (SLT) will be encouraging and supporting the positive use of Information and Communication Technology (ICT) to develop curriculum and learning opportunities in schools and settings. Nevertheless it is essential that the use of ICT and online tools is carefully managed to ensure that all members of the school community are kept safe as well as their data and that risks or dangers are recognised and mitigated.

This template Acceptable Use Policy (AUP) provides a structure which is appropriate to the school e-Safety ethos and approach. The AUP will need to be adapted by the school for a variety of different audiences and for their individual requirements and systems. It should be developed by a member of SLT and must be approved by the Head Teacher and Governing Body. **It is recommended that staff should be actively involved in writing the AUP to ensure it is appropriate and meets the requirements of the establishment.**

### ***Legislation***

Schools may wish to read relevant legislation and information regarding this document and amend the school's AUP accordingly. Schools have a duty of care to safeguard and protect staff under the Health and Safety at Work Act 1974 and the Management of Health and Safety at Work Regulations 1999. Key legislation also includes Section 11 of the Children Act 2004 which places a duty on key persons and bodies to ensure that their functions are discharged having regard to the need to safeguard and promote the welfare of children. Schools may also wish to read and consider the document "Guidance for Safer Working Practice for Adults who Work with Children and Young People" (2009), which contains useful guidance around professional use of technology.

[www.childrenengland.org.uk/upload/Guidance%20.pdf](http://www.childrenengland.org.uk/upload/Guidance%20.pdf)

### ***Data Protection Act 1998***

Schools must also ensure they comply with the Data Protection Act (DPA) 1998. Under the DPA every organisation that processes personal information (personal data) must notify (register with) the Information Commissioner's Office, unless they are exempt. Specific guidance for education establishments, including information on how to register and check notification may be found here:

[http://www.ico.gov.uk/for\\_organisations/sector\\_guides/education.aspx](http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx)

The DPA applies to anyone who handles or has access to information concerning individuals and everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. Schools should have a Data Protection and Security Policy in place to outline the legal responsibilities and actions taken to protect personal data in accordance with the DPA. This may include password safety, use of encryption, use of laptops, email and portable data storage devices (e.g. memory sticks) not sharing login information etc. Schools can read more information from the Information Commissioner's Office: <http://www.ico.gov.uk/>

A Staff AUP is not intended to unduly limit the ways in which members of staff teach or use ICT, but aims to ensure that the school and all members of staff comply with the appropriate legal responsibilities, the reputation of the school is maintained and the safety of all users is ensured. Members of staff are entitled to seek their own legal advice on this matter before signing the AUP.

In order to protect staff members it is essential to have an AUP in place which has been viewed and understood. All employees (including teaching and non-teaching staff) must be aware of the school rules for use of information systems and professional conduct online whether on or off site. Misuse of ICT systems and other professional misconduct rules for employees (whether from Sheffield City Council or other professional bodies) are specific and instances resulting in disciplinary procedures or staff dismissal have occurred.

With internet use becoming more prominent in every day life for personal and professional use, it is important that all members of staff are made aware that their online conduct both in and out of school could have an impact on their role and reputation. Civil, legal or disciplinary action could be taken should they be found to have brought the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities. It is therefore important that the AUP is firmly embedded within the school induction process for all members of staff (including any volunteers, part-time staff or work experience placements). It is also important that all members of staff receive up-to-date and relevant training around this issue on a regular basis. All members of staff should read, understand and sign the AUP before being granted access to any of the schools' ICT systems.

### **Social Media**

Some settings may wish to provide more explicit guidance for staff around use of social networking and email as, even when use of social media sites such as Facebook and Twitter occur in their own time using their own computer, it can leave staff vulnerable to abuse or a blurring of professional boundaries.

Schools must be aware they cannot ban staff from using sites in their own personal time; however they can put in place appropriate guidance and boundaries around staff interaction with pupils (past or present) and parents. It is recommended that any contact with pupils and parents only takes place via school approved communication channels e.g. school email address or the school learning platform so it can be monitored and traced in the case of an allegation or concern. However, schools must recognise that in some cases there may be pre-existing relationships which mean that any "ban" from adding pupils or parents as friends or contacts on personal social networking sites may be difficult to enforce. It is therefore recommended that members of staff are encouraged to make SLT aware of these exceptions in order to protect themselves from allegations or misinterpreted situations.

It is crucial that all members of staff are made aware of the boundaries and professional practices online in order to protect their professional status. Staff should be advised to check

their privacy settings on any personal social media sites they use, however they should always remember that once content is shared online it is possible for it be circulated more widely than intended without consent or knowledge (even if content is thought to have been deleted or privately shared). [A Social Media Policy for schools is available](#)

### ***Use of Equipment***

Settings may also wish to consider adding a statement regarding their policy on staff using school equipment for personal use. Occasional personal use of the school's computers can be beneficial to the development of staff IT skills and to enable staff to maintain a positive work-life balance. However this is at the school's discretion and can be revoked at any time. Any online behaviour and activity by a member of staff whilst using the school systems must be in accordance of the school AUP and any policies relating to staff conduct and personal use must not interfere with the member of staff's duties or be for commercial purpose or gain (unless authorised by the SLT).

### ***Use of Personal Devices***

It is recommended that staff do not use their own devices for school business, such as personal mobile phones to communicate with pupils whilst on educational visits or using the camera/video on their mobile phone. On occasions when the use of a personal camera is necessary, permission should be sought from the Headteacher/SLT. The images should then be transferred to the school network and deleted from the camera.

Schools may also consider providing staff with a written process or chart to follow for reporting any incidents or concerns to ensure that all members of staff are aware of and understand the school's specific safeguarding procedures. **Where the school outsources any ICT services it is essential that an AUP is created as part of the service level agreement and is owned and enforced by both the managed service and the school.**

The Staff AUP should be reviewed regularly (at least annually) and should be revisited and updated in response to any changes, for example after an incident, introduction of new technologies or after any significant changes to the school organisation or technical infrastructure. Any amendments to the AUP should then be communicated to all staff.

The AUP template suggests a range of statements and should be used to develop the schools e-Safety ethos and whole-school approach. This AUP template is suitable for all schools and other educational settings (such as Pupil Referral Units, 14-19 settings and Hospital Schools etc) and we encourage establishments to ensure that their AUP is fit for purpose and individualised for their context. For simplicity we have used the terms 'school' and 'pupils', but wider educational settings are equally relevant.

If schools or settings wish to discuss the use and application of Acceptable Use Policies or any other e-Safety concerns, please contact the E-safety Project Manager, Sheffield Safeguarding Children Board [julia.codman@sheffield.gov.uk](mailto:julia.codman@sheffield.gov.uk) 0114 2736945 or contact the Safeguarding Advisory Service 0114 2053554

## Further Information

- Sheffield Schools and settings can consult with the e-Safety Manager via: [julia.codman@sheffield.gov.uk](mailto:julia.codman@sheffield.gov.uk) or telephone 0114 2736945.
- Training is available via Safeguarding Training Service on 0114 Telephone: 0114 2735430 or email [safeguardingchildretraining@sheffield.gov.uk](mailto:safeguardingchildretraining@sheffield.gov.uk)
- The UK Safer Internet Centre's Professional Online Safety Helpline offers advice and guidance around e-Safety for professionals who work with children and young people in the UK. The helpline provides support with all aspects of digital and online issues such as social networking sites, cyber-bullying, sexting, online gaming and child protection online. Staff can contact the helpline via 0844 381 4772, [helpline@saferinternet.org.uk](mailto:helpline@saferinternet.org.uk) or can visit [www.saferinternet.org.uk/helpline](http://www.saferinternet.org.uk/helpline) for more information.
- "Safer Use of New Technology" is a Kent Safeguarding Children Board (KSCB) document which discusses ideas and FAQs for professionals on how to use technology safely when working with young people. The document can be downloaded from [www.kenttrustweb.org.uk?esafety](http://www.kenttrustweb.org.uk?esafety)
- "Supporting School Staff" is an essential document to help staff understand how to protect themselves online created by Childnet International and DfE: <http://www.digizen.org/resources/school-staff.aspx>
- Teach Today is a useful website which provides useful advice and guidance for staff from industry: <http://en.teachtoday.eu>
- 360 Degree Safe tool is an online audit tool for schools to review current practice: <http://360safe.org.uk/>
- "Guidance for Safer Working Practice for Adults who Work with Children and Young People" (2009) contains useful guidance around professional use of technology. [www.childrenengland.org.uk/upload/Guidance%20.pdf](http://www.childrenengland.org.uk/upload/Guidance%20.pdf)



# Staff ICT Acceptable Use Policy 2013

***As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.***

**This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.**

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites.
- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. (Schools might wish to refer to their Data Security Policy). Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.
- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. Where possible I will use the School Learning Platform to upload any work documents and files in a password protected environment (if appropriate). I will protect the devices in my care from unapproved access or theft.

- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.
- I will respect copyright and intellectual property rights.
- I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.
- I will report all incidents of concern regarding children's online safety to the Designated Child Protection Coordinator (**Emma Hardy**) and/or the e-Safety Coordinator (**Stephen Young**) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to (**Stephen Young**) the e-Safety Coordinator or (**Emma Hardy**) the designated lead for filtering as soon as possible.
- I will request permission to bypass any filtering and/or security systems put in place by the school and I will have checked the site before I take the children to it. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT Support Provider/Team via the Business Manager as soon as possible.
- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.
- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the City Council, into disrepute.
- I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the e-Safety Coordinator Stephen Young or the Head Teacher.
- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

*The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.*

**I have read and understood and agree to comply with the Staff ICT Acceptable Use Policy.**

Signed: ..... Print Name: ..... Date: .....

Accepted by: ..... Print Name: .....

# Parent / Carer Acceptable Use Policy Agreement Template

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *students / pupils* will have good access to ICT to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

## Permission Form

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above *students / pupils*, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will promote positive, safe and responsible behaviour on the internet. I will inform the school if I have concerns over my child's e-safety.

Signed

Date



# Use of Photographs, videos and other images within School

**This applies to all staff, volunteers and students on work placement.**

**There are a number of things that you need to address when using images of people, especially children, some of which is contained in the Data Protection Act 1998:**

- You must get the consent of all parents of children appearing in the photograph or video/DVD image before it is created
- You must be clear why and what you'll be using the image for and who will see it
- If you use images from another agency, you need to check that the agency has obtained informed consent

## **Safeguarding issues:**

- Use equipment provided by the school to take the images and not personal devices
- Download and store images in a password protected area of the school network not on personal computers
- When images are stored on the system they should be erased immediately from their initial storage location e.g. camera
- Don't use full names or personal contact details of the subject of any image you use
- Children and families fleeing domestic abuse may be recognised via photos/images and whereabouts revealed to an abusive partner
- No images of a looked after child should be created or used without prior consent from Children's Social Care
- Don't use images of children in swimming costumes or other revealing dress – this reduces the risk of inappropriate use
- Always destroy images once consent has expired or the child has left your school

## **Consider:**

- Are CCTV (security) cameras sited where they may compromise the privacy of individuals?
- How public are your display boards?
- What is the purpose and audience of video's and DVD's you have created?
- Are all of your images and media securely stored at your school?
- Images on websites, and other publicity can become public and outside your control
- Any implications of using images offsite
- The press are exempt from the Data Protection Act, if you invite them to your premises or event, you need to obtain prior consent from parents of children involved
- Including images from different ethnic groups and those of disabled children
- Check out any copyright implications

The Information Commissioner's Office guidance advises that photographs taken for personal use e.g. by parents at special events, at an education setting are not covered by the Data Protection Act.

## **Useful links/resources:**

- **Photographs and Videos, Information Commissioners Office, at:**  
[http://www.ico.gov.uk/for\\_the\\_public/topic\\_specific\\_guides/schools/photos.aspx](http://www.ico.gov.uk/for_the_public/topic_specific_guides/schools/photos.aspx)



## Sample consent form

# Using images of children in (school name)

**Name of the child's mother/father/carer/guardian:**

**Name of child:**

**Date of birth:**

Occasionally, we may take photographs of the children at our school. We use photographs as evidence of learning, part of observations and development records (learning journeys). We may also use these images in our prospectus or in other printed publications that we produce, as well as on our website. We may also make video/DVD recordings for monitoring events or other educational use.

In the event of our school being visited by the media who may take photographs or film footage of an event, children and young people may appear in these images, which may appear in local or national newspapers, or on televised news programmes.

No personal details to identify a child will be provided with the images.

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make any recordings of your child. Please answer questions 1 to 5 below, then sign and date the form where shown.

**Please return the completed form to the setting as soon as possible.**

- 1) May we use your child's photograph in our prospectus and other printed publications for promotional purposes? Yes/No
- 2) May we put your child's image on our website? Yes/No
- 3) May we record your child's image on video/DVD? Yes/No
- 4) Are you happy for your child to appear in the media? Yes/No
- 5) May we use your child's image in our school newsletter? Yes/No

*Please note that websites can be viewed throughout the world and not just in the United Kingdom where UK law applies.*

**I have read and understood the conditions of use.**

Parent's or guardian's signature:

Name (in block capitals):

Date

**If circumstances change which could impact on your child's safety and security, please inform the School immediately.**

# Mobile phone usage in schools

## General issues

### Possible statements

- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms and toilets.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- Personal mobile phones will only be used during lessons with permission from the teacher.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- All mobile phones and personally-owned devices will be handed in at reception should they be brought into school.

## Pupils' use of personal devices

### Possible statements

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- Pupils will be provided with school mobile phones to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up so that only those features required for the activity will be enabled.



# Questions for Schools

## Consult, monitor and review

- Do we raise awareness and hold discussions on what e-safety is, involving staff, children and young people, governors and parents?
- Do we keep a record of e-safety incidents, according to our agreed definition, and analyse it for patterns – people, places, groups, technologies?
- Do we ask ourselves what makes an e-safe school?
- What is our school doing to ensure that our children and young people do not feel vulnerable and are safe to learn, when engaged in online activities?
- Do we celebrate our successes and draw these to the attention of parents/carers and the wider community?
- Do we consult our staff about their concerns around e-safeguarding issues and their training needs?
- Do we acknowledge and learn from the high level of skills and knowledge of children and young people in the use of new technologies?
- Do we regularly find out children and young people's views on the extent and nature of e-safety issues?

## Support everyone in the school community to identify and respond

- Do we work with staff and outside agencies to identify all potential forms of e-safety incidents?
- Do we actively provide systematic opportunities for developing pupils' skills to develop safe online behaviour?
- Have we considered all the opportunities where this can be addressed – through the curriculum; through corridor displays; through assemblies; through the School Council; through peer support; and through the website and parents' evenings and newsletters?
- Do we ensure that there is support for vulnerable children and young people?
- Do we train all staff to be aware of potential e-safety issues and follow school policy and procedures on e-safety?
- Do our staff feel adequately supported to be able to respond to and manage e-safety related incidents?

## Ensure that children and young people are aware of how and to whom e-safety incidents should be reported and understand that all e-safety concerns will be dealt with sensitively and effectively

- Do we ensure that young people know how to express worries and anxieties about e-safety?
- Do we ensure that all staff, children and young people are aware of the range of sanctions which may be applied against those involved in e-safety misuse?
- Do we involve children and young people in e-safety events, campaigns in school?
- Do we demonstrate that we are aware of the power of peer support? Have we created and publicised schemes of peer mentoring or counselling; buddying or mediation, for example?
- Do we include information about help available in school and the phone numbers of help-lines in the school's student planners?



- Have we made children and young people aware of “how to report abuse”?
- Do we have an e-safety notice board?
- How else do we bring e-safety messages to children and young people’s attention?
- What role does our School Council already play in our e-safety work? How might that involvement be enhanced?
- Do we offer sufficient support to children and young people who have been involved in e-safety incidents?
- Do we work with children and young people who have been involved, or may be seen as being at risk?

**Ensure that parents/carers are aware of e-safety issues and that those expressing concerns have them taken seriously**

- Do we work with parents and the local community to address issues beyond the school gates that give rise to e-safety issues? – particularly with regard to the possible lack of filtering and monitoring of internet access by children and young people out of school and with regard to cyber-bullying incidents
- Do parents know whom to contact if they are worried about e-safety issues?
- Do parents know about our complaints procedure and how to use it effectively?

**Learn from effective e-safety work elsewhere and establish effective collaboration**

- Have we invited colleagues from a school with effective e-safety policies and practice to talk to our staff?
- Have we involved the Sheffield Safeguarding Children Board staff or other local / regional experts in any way?
- Do we have an established link with the police?

# Links to other organisations or documents

The following sites will be useful as general reference sites, many providing good links to other sites:

Sheffield Safeguarding Children Board <http://www.safeguardingsheffieldchildren.org.uk>

Safer Internet Centre: <http://www.saferinternet.org.uk/>

UK Council for Child Internet Safety: <http://www.education.gov.uk/ukccis>

CEOP - Think U Know - <http://www.thinkuknow.co.uk/>

Childnet - <http://www.childnet.com>

Netsmartz <http://www.netsmartz.org/index.aspx>

Teach Today <http://www.teachtoday.eu/>

Internet Watch Foundation – report criminal content: <http://www.iwf.org.uk/>

Byron Review (“Safer Children in a Digital World”)  
<http://webarchive.nationalarchives.gov.uk/tna/+/dcscf.gov.uk/byronreview/>

Guidance for safer working practice for adults that work with children and young people -  
<http://webarchive.nationalarchives.gov.uk/20100202100434/dcsf.gov.uk/everychildmatters/resources-and-practice/ig00311/>

Information Commissioners Office/education:  
[http://www.ico.gov.uk/for\\_organisations/sector\\_guides/education.aspx](http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx)

ICO guidance on use of photos in schools:  
[http://www.ico.gov.uk/youth/sitecore/content/Home/for\\_the\\_public/topic\\_specific\\_guides/schools/photos.aspx](http://www.ico.gov.uk/youth/sitecore/content/Home/for_the_public/topic_specific_guides/schools/photos.aspx)

Ofsted survey: [http://www.ofsted.gov.uk/Ofsted-home/Publications-and-research/Browse-all-by/Documents-by-type/Thematic-reports/The-safe-use-of-new-technologies/\(language\)/eng-GB](http://www.ofsted.gov.uk/Ofsted-home/Publications-and-research/Browse-all-by/Documents-by-type/Thematic-reports/The-safe-use-of-new-technologies/(language)/eng-GB)

Plymouth Early Years E-Safety Toolkit:  
[http://www.plymouth.gov.uk/early\\_years\\_toolkit.pdf](http://www.plymouth.gov.uk/early_years_toolkit.pdf)

Protecting your personal information online:  
[http://www.ico.gov.uk/~media/documents/library/data\\_protection/practical\\_application/protecting\\_your\\_personal\\_information\\_online.ashx](http://www.ico.gov.uk/~media/documents/library/data_protection/practical_application/protecting_your_personal_information_online.ashx)

Getnetwise privacy guidance: <http://privacy.getnetwise.org/>

## Children and Parents

Vodafone Parents Guide: <http://parents.vodafone.com/>

NSPCC: [http://www.nspcc.org.uk/help-and-advice/for-parents-and-carers/internet-safety/internet-safety\\_wdh72864.html](http://www.nspcc.org.uk/help-and-advice/for-parents-and-carers/internet-safety/internet-safety_wdh72864.html)

Google guidance for parents: <http://www.teachparentstech.org/>

E-Parenting tutorials: <http://media-awareness.ca/english/parents/internet/eparenting.cfm>

Practical Participation – Tim Davies: <http://www.practicalparticipation.co.uk/yes/>

Digital Citizenship: <http://www.digizen.org.uk/>

Kent “Safer Practice with Technology”:

[http://kentrustweb.org.uk/CS/community/kent\\_teachers/archive/2009/07/07/safer-practice-with-technology-for-school-staff.aspx](http://kentrustweb.org.uk/CS/community/kent_teachers/archive/2009/07/07/safer-practice-with-technology-for-school-staff.aspx)

Connect Safely Parents Guide to Facebook:

<http://www.connectsafely.org/Safety-Advice-Articles/facebook-for-parents.html>

Ofcom – Help your children to manage the media:

<http://consumers.ofcom.org.uk/2010/10/parental-controls-help-your-children-manage-their-media/>

Mobile broadband guidance: <http://www.mobile-broadband.org.uk/guides/complete-resource-of-internet-safety-for-kids/>

Orange Parents Guide to the Internet: <http://www.orange.co.uk/communicate/safety/10948.htm>

O2 Parents Guide: <http://www.o2.co.uk/parents>

FOSI – Family Online Internet Safety Contract: <http://www.fosi.org/resources/257-fosi-safety-contract.html>

Cybermentors (Beat Bullying): <http://www.cybermentors.org.uk/>

Teachernet Cyberbullying guidance:

<http://www.digizen.org/resources/cyberbullying/overview>

“Safe to Learn – embedding anti-bullying work in schools”

[http://www.anti-bullyingalliance.org.uk/tackling\\_bullying\\_behaviour/in\\_schools/law\\_policy\\_and\\_guidance/safe\\_to\\_learn.aspx](http://www.anti-bullyingalliance.org.uk/tackling_bullying_behaviour/in_schools/law_policy_and_guidance/safe_to_learn.aspx)

Anti-Bullying Network - <http://www.antibullying.net/cyberbullying1.htm>

Cyberbullying.org - <http://www.cyberbullying.org/>

CBBC – stay safe: <http://www.bbc.co.uk/cbbc/help/home/>

## Technology

Kaspersky – advice on keeping children safe - [http://www.kaspersky.co.uk/keeping\\_children\\_safe](http://www.kaspersky.co.uk/keeping_children_safe)

Kaspersky - password advice: [www.kaspersky.co.uk/passwords](http://www.kaspersky.co.uk/passwords)

CEOP Report abuse button: <http://www.ceop.police.uk/Safer-By-Design/Report-abuse/>

Which Parental control guidance: <http://www.which.co.uk/baby-and-child/child-safety-at-home/guides/parental-control-software/>

How to encrypt files: <http://www.dummies.com/how-to/content/how-to-encrypt-important-files-or-folders-on-your-.html>

Get safe on line – Beginners Guide -  
[http://www.getsafeonline.org/nqcontent.cfm?a\\_name=beginners\\_1](http://www.getsafeonline.org/nqcontent.cfm?a_name=beginners_1)

Childnet Parents and Teachers on downloading / music, film, TV and the internet -  
<http://www.childnet.com/downloading/>

Microsoft Family safety software: <http://windows.microsoft.com/en-US/windows-vista/Protecting-your-kids-with-Family-Safety>

Norton Online Family: <https://onlinefamily.norton.com/>

Forensic Software <http://www.forensicsoftware.co.uk/education/clients.aspx>

# Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

## Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

## Data Protection Act 1998

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject’s rights.
- Secure.
- Not transferred to other countries without adequate protection.

## Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

## Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

## Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

## **Regulation of Investigatory Powers Act 2000**

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
  - Ascertain whether the communication is business or personal;
  - Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

## **Copyright, Designs and Patents Act 1988**

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

## **Telecommunications Act 1984**

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

## **Criminal Justice & Public Order Act 1994**

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

## **Racial and Religious Hatred Act 2006**

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

## **Protection from Harassment Act 1997**

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

## **Protection of Children Act 1978**

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

### **Sexual Offences Act 2003**

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

### **Public Order Act 1986**

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

### **Obscene Publications Act 1959 and 1964**

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

### **Human Rights Act 1998**

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

### **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.

SSCB would like to acknowledge YHGfL, SWGfL and Kent County Council for the use of their documentation.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in October 2012. However, SSCB cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.

© SSCB 2012