To Know To Love To Share

# All Saints' & St Richard's Church of England Primary School

# E-Safety and Acceptable Use Policy 2016

| | |
|---|---|
| Implemented | January 2016 |
| Review Cycle | Annual |
| Review Date | September 2016 |

## Introduction

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. E-Safety is a safeguarding issue and therefore all staff are responsible for ensuring our children and school community stay safe when using digital technologies.

It is the responsibility of all persons connected with the school to be vigilant in reporting any e-safety concerns to the E-Safety Leader, Caroline Harvey or in her absence the deputy Designated Safeguarding Lead (DSL).

## Scope:

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated Behaviour and Anti-Bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

## E-Safety throughout the school

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies
- Sound implementation of the E-Safety and Acceptable Use Policy in both administration and curriculum, including secure school network design and use
- Safe and secure broadband from SEGfL including the effective management of Web filtering
- National Education Network standards and specifications

## Roles and Responsibilities:

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

### Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the nominated E-Safety Governor, Mr Liam Backler. The E-Safety Governor will receive regular information about e-safety incidents and monitoring reports.

The role of the E-Safety Governor will include:

- Bi-termly meetings with the E-Safety Leader (3 times a year)
- Bi-termly monitoring of e-safety incident logs (3 times a year)
- Termly monitoring of filtering (6 times a year)
- Reporting to the full governing body bi-termly (3 times a year)

### Headteacher:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community.
- The Headteacher should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff and will ensure that Key Stage Leaders are aware of the flow chart on dealing with e-safety incidents.
- The Headteacher is responsible for ensuring that the E-Safety Leader and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues.

### E-Safety Leader:

The E-Safety Leader at ASSR is Mrs Caroline Harvey. Specific responsibilities include to:

- meet with and report to the E-Safety Governor
- take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school E-Safety policies
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- provide training and advice for staff
- liaise with the Local Authority when necessary
- liaise with the ICT technician
- receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments (see Appendix 2)
- meet bi-termly with the E-Safety Governor to discuss current issues, review incident logs and filtering

### Network Manager:

The school has a managed ICT service provided by East Sussex Local Authority. The Network Manager is responsible for ensuring:

- the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person

## Teaching and Support Staff:

All teaching and support staff have a responsibility for e-safety. They are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current E-Safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP) and ICT Code of Conduct
- they report any suspected misuse or problem to the E-Safety Leader for investigation /action /sanction
- all digital communications with students /pupils /parents/carers are on a professional level and are only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the E-Safety and Acceptable Use Policies
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

## Designated Safeguarding Lead (DSL):

The DSL should be trained in e-safety issues and be aware of the potential for serious child protection /safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

## Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so (Zip it, Block it, Flag it)
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking /use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the *school*'s E-Safety Policy covers their actions out of school, if related to their membership of the school

## 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. The school will take every opportunity to help parents understand these issues through parents' meetings, newsletters, websites and literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- their children's personal devices in the school (where this is allowed)

## E-Safety Audit

| | |
|---|---|
| The policy is available for staff at O:\E-Safety\E-Safety and Acceptable Use Policy 2016.doc | |
| The policy is available to parents on the school website at www.assr.org.uk | |
| The Designated Safeguarding Lead (DSL) is: Caroline Harvey | |
| The E-Safety Leader is: Caroline Harvey | |
| This policy has been reviewed  staff and Governors | |
| All staff sign an ICT code of Conduct on appointment? | Yes |
| Parents sign and return an agreement that their child will comply with the School E-Safety Rules | Yes |
| School E-Safety rules been set for pupils | Yes |
| These E-Safety rules are displayed in all rooms with computers | Yes |
| Internet access is provided by an approved educational Internet Service Provider and complies with DfE requirements for safe and secure access. | Yes |
| Personal data collected is stored and used according to the principle of the Data Protection Act. | Yes |

## 1. Writing and Reviewing the E-Safety Policy

The E-Safety Policy is part of the School Improvement Plan (ScIP) and relates to other policies including those for ICT, Anti-Bullying and Safeguarding. The school has appointed the Headteacher as the E-Safety Leader.

- Our E-Safety Policy has been written by the school, following East Sussex E-Safety Guidance and guidance from the swgfl. It has been agreed by staff and approved by governors.
- The E-Safety Policy was devised by: Caroline Harvey

## 2. Teaching and Learning

### Why Internet use is important?

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.

### Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. Refer to Appendix 3 – Teaching, Learning and the Internet.

### Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils in KS1 and KS2 will be taught about E-Safety each term following the ESCC schemes of work and the computing requirements of the National Curriculum. Pupils will be taught that the following are not permitted within school and the community:

    - displaying offensive messages or pictures
    - using obscene language, harassing, insulting or attacking others (whether on or off school premises or within/outside of normal school hours)
    - damaging computers, computer systems or computer networks
    - violating copyright laws
    - using other people’s logins and/or passwords, trespassing in others’ folders, work or files
    - intentionally wasting limited resources
    - through the curriculum pupils are also taught the importance of not involving themselves in any of the above actions in or outside of school

- The school will take part in the nationally recognised Safer Internet Day annually and then use the guidance and materials to support E-Safety teaching and learning within school.

## Managing Internet Access

### Information System Security

- School ICT systems, capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with ESCC.

### E-mail and Messaging

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communications, or arrange to meet anyone without specific written permission from their parents and teacher.
- E-mails to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Message content should not cause offense or be likely to cause offense.
- Attachments sent to pupils should not be opened unless a staff member gives permission.
- Pupils should be taught to scan attachments before opening.
- Any incidents involving inappropriate use of e-mail should be dealt with by the class teacher in conjunction with the E-Safety Leader. Parents should be informed.
- Pupils should be reminded to write polite, friendly, non-offensive messages and e-mails.

### Published content on the school website

- The contact detail on the school website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

### Publishing pupil's images and work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.
- Photographs that include pupils will be selected carefully to ensure the images are suitable for sharing on the website.
- Pupil image file names will not refer to the pupil by name.
- Pupils' full names will not be used anywhere on a school website or other on-line space particularly in association with photographs.
- Work can only be published with the permission of the pupils.

## Social networking and personal publishing

- The school will block/filter access to social networking sites apart from moderated social networking sites e.g. SuperClubsPlus.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friend or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites in and out of school.

## Managing Filtering

- The school will work with the LA, DfE and RM Safety Net to ensure systems to protect pupils are reviewed and improved.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- If staff or pupils come across unsuitable on-line materials an online incident record should be made and reported to the E-Safety Leader. Guidance on how to deal with incidents can be found in the ESCC Incident Guidance for Staff (Appendix 1).

## Internet use at home

- Parents and carers will be advised to contact their own Internet Service Provider to explore home filtering and child controls.
- Parents are advised not to allow their child unsupervised access to the internet.
- Parents will be provided with information about keeping their children safe on line at least annually. Up to date information will be sent out each February to raise awareness of Safer Internet Day and information for parents.

## Managing Video Conferencing

- Video conferencing will be booked in advance between schools or through a trusted provider under the strict supervision of school staff.
- Teachers must ensure video conferencing equipment is switched off when not in use and not set to answer.
- Ensure that video conferencing contact is not put on the School website.
- Ensure that parents and carers have given express permission for their children to take part in video conferences.
- Ensure that staff only are issued with a unique log on and password details for educational video conferencing services.
- Ensure that recorded material is stored securely.

## Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The senior leadership team should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during lessons or dedicated teaching time in class.

- The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The use by pupils of cameras or tablets will be kept under review.
- Staff will use the school phone system where contact with pupils is required or where mobile phones are used to capture photographs of pupils.

## 3 Policy Decisions

### Authorising Internet Access

- All staff must read and sign the ICT Code of Conduct for Staff and Acceptable Use Statement before using any ICT resource.
- At Key Stage 1 access to the internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form for use of the internet in school.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

### Assessing Risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor ESCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the E-Safety Policy is adequate and that its implementation is effective.

### Handling E-Safety Complaints

- Complaints of Internet misuse will be dealt with initially by the E-Safety Leader in accordance with Appendix 1 – E-Safety Incident Flow Chart.
- All E-Safety incidents will be recorded in the format shown in Appendix 2. This is known as the E-Safety Incident Record.
- A copy of the E-Safety Incident record will be given to the Headteacher, the DSL (if not the same person) and ESCC. One copy will be stored in the pupil or staffs' file. One copy will be kept by the E-Safety Leader.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a safeguarding nature must be dealt with in accordance with the school child protection and safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions may be held with the police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.
- When handling complaints about the way the school has dealt with an E-Safety incident, all complaints will be dealt with in accordance with the Compliments, Concerns and Complaints Policy.

### Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This sometimes means that staff may want to bring their own digital devices into school to provide greater freedom of choice and usability.

However, there are a number of e-safety considerations that need to be taken into account if staff wish to do this. The following procedures need to be followed if a member of staff wishes to bring in their own digital device so that vulnerabilities are not created within the school's security:

- The ICT Code of Conduct and Acceptable Use polices still apply when staff are using their own devices at school.
- Data Protection principles must be adhered to e.g. personal information and pupil images must not be stored on staff's own devices
- Where possible devises should be operated through the school filtering system e.g. be logged on to the school wi-fi
- All users will use their username and password and keep this safe

## 4 Communications Policy

### Introducing the E-Safety Policy to pupils

- E-Safety rules will be displayed in all rooms where computers are used and discussed with pupils regularly (see Appendix 4 – E-Safety Rules).
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- E-Safety Training will be embedded in the Computing Scheme of Work and PSHEe Curriculum.

### Staff and the E-Safety Policy

- All staff will be given the School E-Safety Policy and have its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff are required to sign the ICT Code of Conduct for Staff (Appendix 5).
- Breaches of the ICT Code of Conduct for Staff will be dealt with in accordance with the flow chart in Appendix 1.
- A staff meeting will be arranged to raise awareness of E-Safety.
- New staff, as part of their induction pack, will be given an up-to-date copy of the E-Safety and Acceptable Use Policy.

### Enlisting parents' support

- Parents and carers attention will be drawn to the School E-Safety Policy in newsletters and by sending out E-Safety updates via the school newsletter.
- The school will maintain a list of e-safety resources for parents and carers.
- The school will ask all new parents to sign the parent/carers Agreement Form for Internet Access, Children's Image Use and Web Publication when they register their child with the school.

## Data Protection

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

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for any longer than necessary or for the purposes other than it was collected
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing"
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- It has clear and understood arrangements for the security, storage and transfer of personal data

Staff must ensure that they:

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

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

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

## 5 Staff Acceptable Use Policy

### Introduction:

Computers and emerging technologies are in integral part of our daily lives and the aim of this policy is to ensure that it is used safely and effectively to support children's learning and support staff in their professional roles. The "computer system" is owned by the school and refers to all computers and associated equipment belonging to the school, whether part of the school's integrated network, stand-alone or taken offsite. The computer system is provided for staff to use primarily for educational and operational purposes, but also on occasion for personal use. All users should ensure that these systems are used responsibly.

ASSR actively promotes the use of ICT and digital technologies to support children's learning and enhance staff's professional development. The internet and World Wide Web are amazing spaces and technologies for us to explore with the children. However, it is important for all staff to take a moment to recognise not only the benefits that technology provides, but also the potential 'risks' to ensure the safety of all.

### Equipment:

- Equipment provided to staff by ASSR should be used and stored securely. Any loss must be reported immediately to the Headteacher or school bursar. Particular attention should be made with laptops and IPad which are particularly susceptible to theft or loss.
- Staff should not leave laptops and IPads unattended, and when transporting them between home and school they should not be visible e.g. in a motor car
- Any faults with school equipment should be reported immediately to East Sussex ICT support via telephone or the online reporting tool. A link is provided on all laptops to support staff to report any problems.
- All personal mobile devices (e.g. laptop, mobile phone, tablet, camera, memory stick) must be scanned and ensured to be virus free before connecting to the school network.
- No modifications must be made to school equipment, any requests for modifications must be made to the school ICT technician who will authorise and implement any acceptable modifications.
- The provision of equipment to staff is primarily for school related business. Any personal use must be in accordance with the guidelines laid out in this policy.
- Staff laptops, or other devices assigned to staff by the school must only be operated by them. It is inadvisable to permit family members or anyone else to operate the equipment.
- Members of staff using laptops at home need to ensure they have adequate insurance in place.
- Staff should adhere to the school internet access policy statement when using school laptops at home.

### Personal and Professional Safety and Security

- Members of staff are required to use "strong" passwords when accessing the school network. Passwords should contain a mixture of letters, numbers and punctuation characters.
- Users must never disclose their usernames or passwords to anybody. A supply login is available for use by supply teachers and staff must ensure that anything needed by the supply teacher is available through this login.
- It is not permissible to use another user's credentials to access the school network.
- No attempt should be made to alter security settings as this may put the network at risk.

- Hacking or deliberate attempts to access restricted areas of the network is not permissible.
- Whilst documents stored on your home drive (H:) is personal there may be exceptional circumstances (sickness, disciplinary matters) when the headteacher considers it essential that your files and electronic communication is accessed. The headteacher will log this request with the school's ICT provider.

### Information and Data Security

It is recognised that teachers need to hold and share a large amount of data pertaining to pupils. The Data Protection Act (1990) requires that all data is held securely, accessed only in accordance with the provisions of the Act and transferred in a secure manner.

- Sensitive information should not be stored on a laptop or other mobile device. This data should be stored on your home (H:) drive, staff (O:) drive or office (J:) drive which is not local to the machine.
- Personal details, including assessment information and contact details should not be stored on a laptop or removable media e.g. memory stick.
- All teaching staff are provided with an encrypted remote access key to enable staff to access the school network remotely. This removes the need to store sensitive information on a laptop. The remote access key can also be used as a memory stick if needed as it is password protected.
- Personal data must not be emailed unless held in an encrypted attachment. Secure mail can be used to send personal information via e-mail.
- Pupils must not be granted unattended access to staff laptops or workstations e.g. office computers.

### Internet and Email

Whilst access to the internet is provided primarily for educational and operational purposes, ASSR recognises that there are times staff may need to use the internet for personal use. However this should never disrupt staff duties. Any online activity should in no way compromise your professional responsibility or bring ASSR into disrepute. Any abuse or excessive personal use of e-mail and or internet facilities will be dealt with through the disciplinary procedure.

### Email:

- No data covered by the Data Protection Act (1990) may be sent in an unencrypted format via email.
- Members of staff have been provided with a school email address for the sole purpose of communication with colleagues and school related external parties. Personal email accounts should be used for all personal communication.
- Staff must not use their own personal email accounts to communicate with parents /pupils.
- Communication via email should always be in a polite and professional manner and should not be aggressive or inappropriate in tone. Emails must not contain offensive, aggressive or inappropriate language.
- The attachment and transmission of inappropriate, obscene, unlawful or abusive material is not acceptable under any circumstances.
- Staff should immediately report any inappropriate emails to the headteacher.
- Posting anonymous messages and forwarding chain letters is forbidden;
- Downloading attachments to emails should only take place where you have requested these attachments and are therefore certain of their origin.
- Children are not to be given individual e-mail addresses in school.

### Internet Access:

All Internet activity should be appropriate to staff professional activities or the children's education. It has been drawn up to protect all parties; the students, the staff and the school.

- Large, excessive downloads are not permitted unless authorised by the headteacher.
- Using the internet/network to obtain, send, store, print, display or transmit material which is obscene, abusive or unlawful will not be tolerated.
- Users must respect the ownership rights of materials and abide by copyright laws.
- To ensure the safety of users ASSR may monitor the use of ICT systems including email and other digital communication.
- Limited personal use of the internet is permissible during lunchtime or outside of directed time.
- The use of media streaming websites e.g. YouTube, IPlayer restricted to school-related purposes.
- Staff must not circumnavigate filtering or security features on the network.
- Children must not be given unsupervised access to the Internet. For the purposes of this policy, "supervised" means that the user is within direct sight of a responsible adult.

### Social Network:

Staff should refer to the Social Media Policy for further information and guidance on using social networking sites.

### Mobile Phones:

- Staff should not provide their home or mobile telephone number to pupils.
- Pupils' and parents' telephone numbers should not be stored on a personal mobile phone.
- Still images or video footage of pupils should not be taken or stored on a personal mobile telephone.
- Mobile telephones must not be used during directed time, except on school trips when being used for the express purpose of contacting school.

### Accountability:

I understand that this Staff Acceptable Use Policy applies not only to my professional conduct and related work at All Saints' and St Richard's Church of England Primary School, but is also applies to my use of personal equipment or in situations related to my employment at ASSR.

I understand that if I fail to comply with this Agreement, I could be subject to disciplinary action or in the event of illegal activities the involvement of the police.

Signed: ______________________________

Date: ______________________________

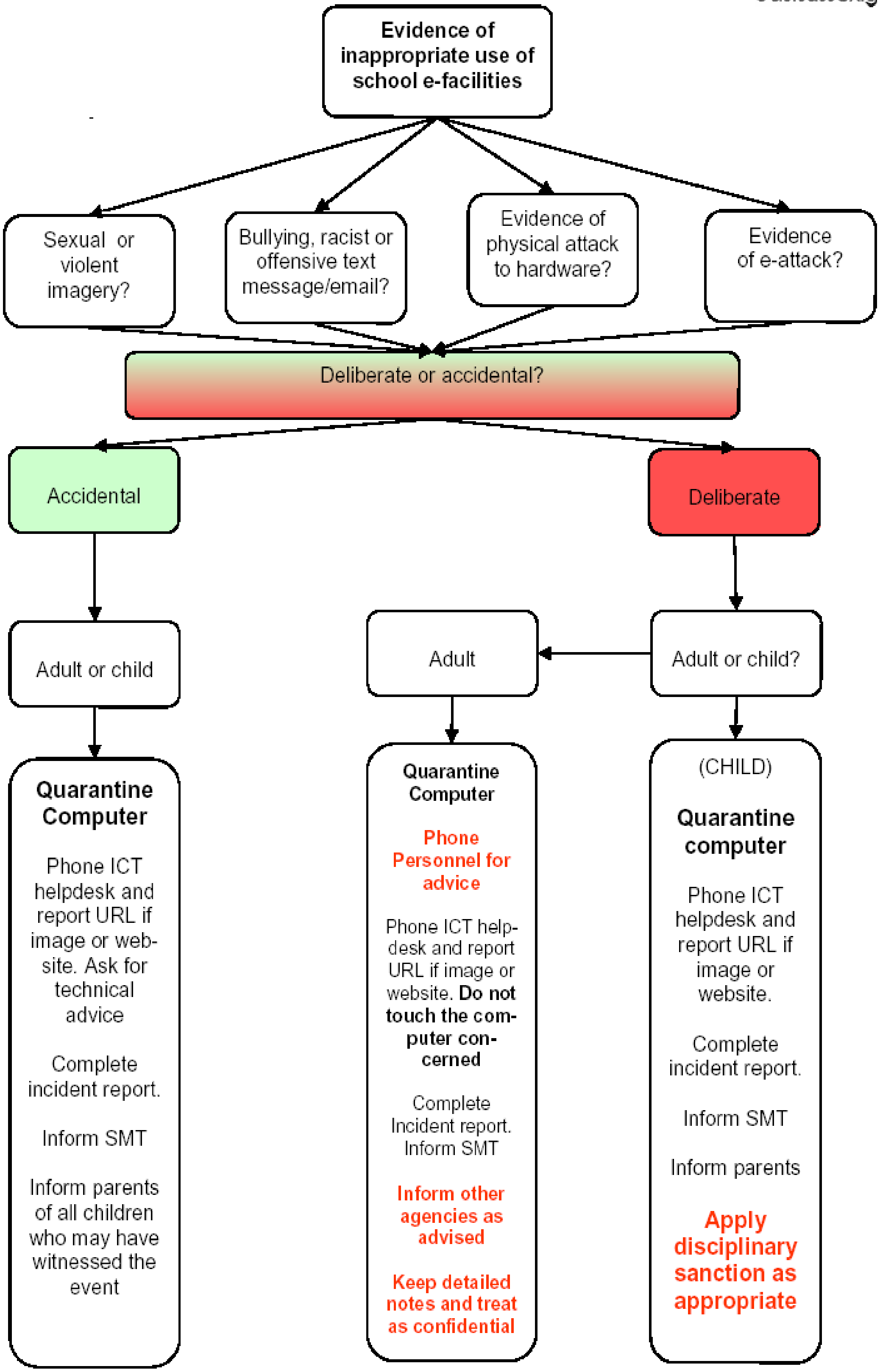
### Monitoring and Review:

This policy will be reviewed annually or sooner if deemed necessary or if relevant new guidance needs to be taken into account.

Date: January 2016 Review: September 2016

East Sussex County Council
eastsussex.gov.uk

## E–safety incident guidance for staff



Evidence of inappropriate use of school e-facilities

Sexual or violent imagery?

Bullying, racist or offensive text message/email?

Evidence of physical attack to hardware?

Evidence of e-attack?

Deliberate or accidental?

Accidental

Adult or child

**Quarantine Computer**

Phone ICT helpdesk and report URL if image or website. Ask for technical advice

Complete incident report.

Inform SMT

Inform parents of all children who may have witnessed the event

Deliberate

Adult or child?

Adult

**Quarantine Computer**

**Phone Personnel for advice**

Phone ICT helpdesk and report URL if image or website. **Do not touch the computer concerned**

Complete Incident report. Inform SMT

**Inform other agencies as advised**

**Keep detailed notes and treat as confidential**

(CHILD)

**Quarantine computer**

Phone ICT helpdesk and report URL if image or website.

Complete incident report.

Inform SMT

Inform parents

**Apply disciplinary sanction as appropriate**

## Appendix 2: E-Safety Incident Record

| | | | | | |
|---|---|---|---|---|---|
| **E-safety incident** | | | **Date** | **Time** | |
| **Name of member of staff (Discovering the incident)** | | | | | |
| **Child(ren) involved. (Or other adults if no children involved)** | | | | | |
| **Nature of incident** | Accidental access to Inappropriate material | Intentional access to inappropriate material | Cyber Bullying | Grooming | Other |
| **Details** | | | | | |
| | | | | | |
| **The event occurred** | During a lesson | In unsupervised time | Outside school hours | | |
| **Does the even warrant direct Police involvement? (YES if…)** | Grooming | Violent image(s) | Pornographic image(s) | Other criminal activity | |

| | | | | | |
|---|---|---|---|---|---|
| **Head Teacher/Deputy Head** | | | | | |
| **(Staff)** | Personnel Contact made with | Recommended action | Action applied | C o Govs | |
| **Other** | | | | | |
| **Children** | Contacted Parents | Date | | Time | |
| | Interviewed Parents/ Carers | (Append notes of interview) Treat as Pink Minute | | | |
| | | | | | |
| | | | | | |
| **File FOUR copies** | Top Copy HT | Second Copy Child Safety Officer | Third Copy Child's file | Personnel File | ESCC |

## Appendix 3: Teaching, Learning and the Internet

| Possible T & L Activities | Key E-Safety Issues | Relevant Websites |
|---|---|---|
| Creating web directories to provide easy access to suitable websites. | Parental consent should be sought.<br>Pupils should be supervised.<br>Pupils should be directed to specific, approved on-line materials. | Web directories e.g.<br>Ikeep bookmarks<br>Webquest UK<br>Kent Learning Zone<br>The school / cluster VLE |
| Using search engines to access information from a range of websites. | Filtering must be active and checked frequently.<br>Parental consent should be sought.<br>Pupils should be supervised.<br>Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with. | Web quests e.g.<br>Ask Jeeves for kids<br>Yahooligans<br>CBBC Search<br>Kidsclick |
| Exchanging information with other pupils and asking questions of experts via e-mail or blogs. | Pupils should only use approved e-mail accounts or blogs.<br>Pupils should never give out personal information.<br>Consider using systems that provide online moderation e.g. SuperClubs Plus. | RM EasyMail<br>SuperClubs Plus<br>School Net Global<br>Kids Safe Mail<br>Kent Learning Zone<br>Cluster Microsite blogs |
| Publishing pupils' work on school and other websites. | Pupil and parental consent should be sought prior to publication.<br>Pupils" full names and other personal information should be omitted.<br>Pupils" work should only be published on „moderated sites" and by the school administrator. | Making the News<br>SuperClubs Plus<br>Headline History<br>Kent Grid for Learning<br>Cluster Microsites<br>National Education Network Gallery |
| Publishing images including photographs of pupils. | Parental consent for publication of photographs should be sought.<br>Photographs should not enable individual pupils to be identified.<br>File names should not refer to the pupil by name.<br>Staff must ensure that published images do not breach copyright laws. | Making the News<br>SuperClubs Plus<br>Learninggrids<br>Museum sites, etc.<br>Digital Storytelling<br>BBC – Primary Art<br>Cluster Microsites<br>National Education Network Gallery |
| Communicating ideas within chat rooms or online forums. | Only chat rooms dedicated to educational use and that are moderated should be used.<br>Access to other social networking sites should be blocked.<br>Pupils should never give out personal information. | SuperClubs Plus<br>FlashMeeting |
| Audio and video conferencing to gather information and share pupils' work. | Pupils should be supervised.<br>Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers. | FlashMeeting<br>National Archives "On-Line"<br>Global Leap<br>JANET Videoconferencing Advisory Service (JVCS) |

Appendix 4:

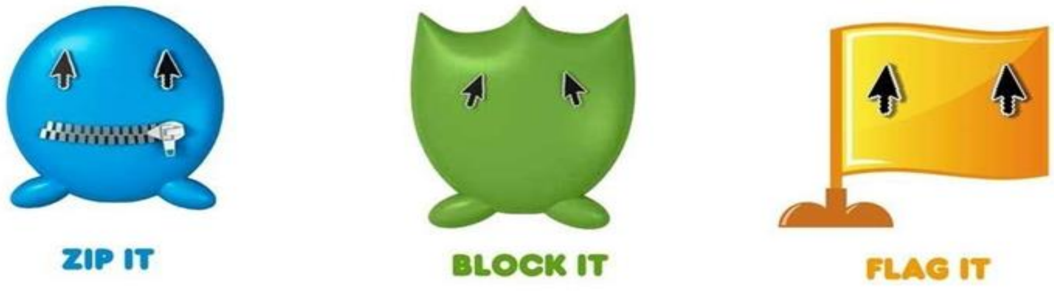
## EYFS and Key Stage 1 Acceptable Use Rules

# 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 polite and friendly messages<br>HELLO! |
| E | If I see something I don't like on a screen, I will always tell an adult. |

## Key Stage 2 Acceptable Use Rules:

| Think then Click |
|---|
| We ask permission before using the Internet. |
| We only use websites that our teacher has chosen. |
| We immediately close any webpage we are not sure about. |
| We only e-mail people our teacher has approved. |
| We send e-mails that are polite and friendly. |
| We never give out personal information or passwords. |
| We never arrange to meet anyone we don't know. |
| We never open e-mails sent by anyone we don't know. |
| We do not use Internet chat rooms. |
| We tell the teacher if we see anything we are worried about. |



**Appendix 5:**

## All Saints' and St Richard's Church of England Primary School

# Staff Code of Conduct for ICT

**To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this Code of Conduct. Members of staff should consult the school's E-Safety and Acceptable Use Policy for further information and clarification.**

- I understand that it is a criminal offence to use a school ICT system for any purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, tablets, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the headteacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the E-Safety Leader, the Designated Safeguarding Lead (DSL) or Headteacher.
- I will ensure that electronic communications with pupils including email, instant message (IM) and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

**The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound**.

**I have read, understood and accept the Staff Code of Conduct for ICT.**

**Print Name:** ______________________________

**Signed:** ______________________________

**Date:** ______________________________