E-Safety Policy

'Every Child, Every Chance, Every Day'

Reviewed By	Russell Hack	Policy Owner	May 2018
Approved By	Annette Hixon & Cate Gregory	Head of School	June 2018
Ratified By	Peter Gould	Governor	June 2018
NEXT REVIEW			May 2020

E-Safety Vision

Shirley Infant and Junior Schools aim to foster an e-safe culture in which issues of e-safety are discussed openly and honestly. We alert our users of potential risks and we encourage the children to develop their own sets of safe and responsible behaviour through computing sessions, discrete e-safety sessions, circle times and by demonstrating positive behaviour both inside and outside school. We appreciate that e-safety is primarily a safeguarding issue for which all staff are responsible (UNICEF, Article 3, 17 27, 19).

Below, we have identified a number of e-safety risks and issues. We aim to avoid these risks and achieve e-safety for our children and staff in three ways. Firstly, through effective policy and practice outlined in this document (including the Acceptable Use Policy and Social Networking Policy). Secondly, by a secure and reliable technical infrastructure, and thirdly, through education and training for all ICT users. Details of these are set out below.

E-safety Risks and Issues

We have identified the following examples of risks and issues which may arise to threaten the e-safety of our children and staff:

Content

- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material such as that inciting violence, hate or intolerance
- Exposure to inappropriate lifestyle material, such as that including pro-anorexia, self-harm etc.
- Exposure to illegal material, such as images of child abuse
- Downloading of copyrighted materials, e.g. music and films
- Plagiarism

Contact

- Grooming using ICT, leading to sexual assault and/or child prostitution
- Grooming using ICT, leading to extremism, terrorism or the support of terrorism (PREVENT 2015)
- Bullies using ICT (e-mail, mobile phones, chat rooms etc.) as a way to torment their victims
- Children and young people self-publishing information – sometimes inappropriately – about themselves and therefore putting themselves at risk

Commerce

- Exposure to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams

Acceptable Use Policy

The schools' Acceptable Use Policy and pupil 'e-safety rules' detail the way in which the school's ICT facilities may and may not be used by staff and children. This is shared with parents and carers to ensure that good practice is extended beyond use in school.

Infrastructure and Network Practice

Within Jefferys Education Partnership, firewall and virus protection are provided for all computers connected to the school's network. Our anti-viral software is checked by our Network Technician and is automatically updated on all equipment as necessary, to maintain protection.

Filtering and content control is similarly provided by Upper Shirley High for all computers and iPads connected to the school network using Smoothwall. This uses a nationally approved database of keywords and URLs which it filters. If concerns are raised about particular keywords and URLs, these can be forwarded to our Network Technician via the school emailing facility.

This technical infrastructure is further secured by good network practice by all users. This includes the following safeguarding procedures:

- Each member of staff has their own personal log-in and password
- Passwords should be strong (a minimum of 7 characters including both numbers and characters) and changed on a regular basis
- Unattended workstations should be logged off/locked
- All removable media and e-mail attachments must be virus checked before being used/viewed on the network

Education and Training

All members of staff are aware of the need for good network practice and have read and agreed to the school's Acceptable Use Policy. All staff will take part in annual training sessions regarding e-safety as required and the E-safety Leader will keep staff informed of new developments. Staff are fully informed as to how they should respond to e-safety incidents as outlined below.

All parents must agree to an e-safety contract when joining Shirley Infant School and Shirley Junior School. New children will receive a copy of our e-safety rules when they join our schools, and all children receive a copy of these annually.

Each year group will learn about the risks and issues surrounding e-safety in an age-appropriate way. They will take part in lessons and circle times where e-safety in the key focus. Teachers will deliver e-safety lessons in accordance with the scheme of work.

All of the school's computers are in public areas and the ICT suite is open access to ensure a staff member can easily monitor use at all times. Our iPads are also only used under close supervision. Unsupervised access to the internet is not allowed.

Due to the strong emphasis on home access to the internet as well as increased use made of electronic communication, we recognise that parents must be made aware of the importance of e-safety. Parents are encouraged to discuss the e-safety contract with their children before signing and enforce our e-safety rules which apply at home as well as in school. Through our annual workshop, parents are made aware of agencies and websites which they may find useful when learning about e-safety or in tackling the issue with their children.

Children should not bring mobile phones into school unless agreed by the head teacher for valid reasons. This is to prevent the possibility of pupils' access to internet sites that may be unsafe.

Responding to E-safety Incidents

Responses to e-safety incidents will differ depending on

1. the severity of the incident and
2. the person or persons concerned (staff member, child or parent).

Minor incidents involving misuse of ICT by pupils should be closely monitored by staff, such as an incident such as using another child's login and password. The class teacher or E-safety Leader should react proactively to any emerging trends. In the first instance, the pupil will receive a verbal warning and the incident will be documented. Further infractions will be recorded, parents may be notified and other appropriate action may be taken.

Online content is filtered by Upper Shirley High's Smoothwall. However, such software is never 100% effective. There remains a small possibility that children may inadvertently or deliberately have access to age-inappropriate materials. All children understand that when such e-safety incidents occur, they must immediately seek help from a trusted adult. It will be a disciplinary matter if a child has deliberately accessed, printed or shared such inappropriate material. The child's parents will be contacted and access to the internet and school network may be restricted. The E-safety Leader will monitor and keep a record of such incidents. Some records will be kept in our safeguarding file. Where incidents are reported to individual teachers, teachers should take immediate steps to ensure that the content cannot be viewed by other children. This may include closing a laptop or switching off a monitor. As soon as possible, the URL must be recorded and passed to the E-safety Leader to be reported to the Network Technician.

In the event of a serious incident occurring in school, including the storage of illegal or indecent material, the police will be contacted. The computer(s) concerned should remain untouched until advised by the police.