E- safety policy

Author, date and title	Reviewed on	Next review due date	Statutory Requirement
Shillington and Stondon Lower schools 2015	February 2020	February 2023	N

As Values Schools, Shillington and Stondon Lower schoolsand Stondon Lower ensures that all its policies, principals and practices adhere to the Values Education ethos.

We are committed to recognising, valuing and respecting the diversity of our schools' communities. We adhere to the Local Authority's Equal Opportunities Policy and the Equality Duty 2010. We welcome all members of the schools' communities irrespective of race, ethnic or national origins, religious and political beliefs, gender, disability, sexuality, age, marital status and linguistic ability. We will ensure equality and value diversity, and address any unfair treatment, discrimination and prejudice.

All our schools' policies include the Pixie class (Shillington) and the before and after school club (Stondon).

Head Teacher: Date: 26/02/2020

Chair of Governors: Lee Fitzpatrick Date: 26/02/2020

Rationale

Shillington and Stondon Lower schools believe that digital technologies are integral to the lives of young people both within school and outside of school. The Internet and other technologies are powerful tools which open up new opportunities. Electronic communication promotes effective teaching and learning through the multiplicity of digital and information applications. All young people have an entitlement to access such technologies, to enhance motivation and engagement and thus facilitate continued improvements in standards across all curriculum areas. The requirement to ensure that young people are able to use technologies appropriately and safely should be addressed as part of the wider duty of care to which all those who work in schools are bound. This e-safety policy should ensure safe and appropriate use. The implementation of this strategy involves all stakeholders in the school community.

Aims

- To provide children with quality Internet access as part of their learning experience fit for the 21st century
- To ensure that ICT is used safely and responsibly and that risks related to ICT use are properly managed
- To keep children safe and teach children about e-safety
- To inform users of the procedures and sanctions for misuse of any technologies either within or beyond the school setting.

Guidelines

Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The World Wide Web
- E-mail
- Instant messaging often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio/audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites
- Video broadcasting sites
- Chat rooms
- Gaming sites
- Music download sites
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down ‘Office’ applications
- On-line learning resources
- Apps
- Other mobile devices including tablets and gaming devices
- Online Games

- Learning Platforms and Virtual Learning Environment

The staff and governors feel they have a duty to ensure that children have a working understanding of how to keep themselves safe whilst using these applications and work towards developing this understanding when using the Internet in school.

Internet Use

Pupils

- Pupils will be taught what Internet use is acceptable and what is not 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.
- Pupils will be shown how to publish and present information to a wider audience.
- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- All pupils must read and sign the school AUP before using any school ICT resource.
- The school will maintain a current record of all pupils who are granted access to school ICT systems.
- Pupils may only use approved e-mail accounts at the school.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils will be advised never to give out their personal details of any kind which may identify them, their friends or their location.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Pupils will be advised that the use of social network spaces outside school brings a range of dangers for primary age pupils.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- If pupils come across unsuitable on-line materials, they should report this to their teacher.

Parents

- Parents and carers attention will be drawn to the e-Safety and acceptable use of IT in newsletters, the school prospectus/handbook and on the school website.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.
- Parents will be advised that the use of social network spaces outside school brings a range of dangers for primary age pupils.
- Parental permission must be to enable the publication of photos

Staff

- All staff will be given the school e-Safety Policy and its importance explained.
- All staff must read and sign the staff school Acceptable Use Policy before using any school ICT resource.

- The school will maintain a current record of all staff who are granted access to school ICT systems.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior leadership and work to clear procedures for reporting issues.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- If staff come across unsuitable on-line materials, the site must be reported to the Computing Subject Leader.
- Recognise that incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- With regard to the school website, the Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website will not publish staff or personal pupil contact information; the contact details given should be for the school office.
- Staff will ensure that group photos rather than full face photos of individual children be used in all publications including the website
- Pupils' full names will not be used anywhere on the school website or publication, particularly in association with photographs.

Additional adults e.g. governors, visitors

- Any person not directly employed by the school will be asked to sign on using a guest log on and access the guest wifi. "acceptable use of school ICT resources" before being allowed to access the internet from the school site.

IT Technician

- Will review school ICT systems security regularly.
- Update virus protection regularly
- Discuss security strategies with the Local Authority.
- In conjunction with the Headteacher, will control access to social networking sites and consider how to educate pupils in their safe use.

Handling e-safety complaints

- Complaints of Internet misuse must be reported to the Computing Subject Leader and Head teacher and will be dealt with accordingly.
- All e-safety incidents will be recorded in the head teacher's secure hard bound incidents log and reported to Governors via the head teacher's report.
- Incidents of Internet misuse by children will be dealt with in line with the school's Promoting Positive Behaviour Policy following the schools' behaviour systems as appropriate.
- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Embedding the Policy

- e-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.

- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in e-safety will be developed, based on CEOP resources for pupils and recommended by the LSCB or Local Authority for staff.

Roles and Responsibilities

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. Reported incidents will be detailed through the Head teacher report/Key Performance Indicators at termly Full Governing Body meetings. The Governor for Safeguarding undertakes a school visit termly and e-safety is audited as part of the visit.

Head teacher and Senior Leaders

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head teacher and Computing Subject Leader, with the support of Governors, aims to embed safe practices into the culture of the school.
The Head teacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Computing Subject Leader.
The Head teacher and (at least) another member of the Senior Leadership Team 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. (Annex B and relevant Local Authority HR disciplinary procedures).
The Head teacher / Senior Leaders are responsible for ensuring that the Computing Subject Leader and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
The Senior Leadership Team will receive regular monitoring reports from the Computing Subject Leader and IT technician

Designated Senior Person for Safeguarding

This person 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
Any concerns regarding e-safety should be reported to the Designated Senior Person for Safeguarding (DSP). The DSP should determine what action is required and who to involve e.g. parental involvement, referral and advice from Central Bedfordshire 'Access Hub'. The DSP will keep records of such occurrences.

Computing Subject Leader

It is the responsibility of the Computing Subject Leader to:
• ensure that they keep up to date with E-Safety issues and guidance through liaison with the Local Authority, attendance at PSG meetings and through organisations such as Becta and The Child Exploitation and Online Protection (CEOP).

• ensure the Head teacher, senior management and Governors are updated as necessary.
• liaise with the IT technician
• provide training and guidance for staff in e-safety

School Business Manager/IT support

• monitors internet activity and usage
• ensures that the school's technical infrastructure is secure and not open to misuse of malicious attack
• ensures that users may only access the networks and devices through a password enforced protection procedure
• ensures appropriate blocks are in place to secure as best access to appropriate websites
• monitors internet activity and usage
• maintains a log of incidents to inform future e-safety developments in partnership with the Computing Subject Leader
• liaises with the Computing Subject Leader with regards to e-safety, driving improvements and changes, policy making

Teachers and Support Staff

Are responsible for ensuring that:
• they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
• they have read, understood and signed the Staff Acceptable Use Policy (AUP)
• they report any suspected misuse or problem to the Head teacher / Senior Leaders/ Computing Subject Leader / IT Technician for investigation / action / sanction
• all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
• e-safety issues are embedded in all aspects of the curriculum and other activities and opportunities to embed key messages are built into daily classroom life
• pupils understand and follow the E-safety and acceptable use policies
• in lessons/assemblies 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

Children

Children are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy. They;
• need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
• will be expected to know and understand the safe use of mobile devices and computing hardware/software
• should be aware of the use of images and cyber-bullying

Parents and 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 newsletters, letters, parent information sessions, website and information about national / local e-safety campaigns / literature.

Named Responsibilities

The Computing Subject Leaders are: Fiona Sharpe (Shillington) and Sarah Comerford (Stondon)
The IT Technical support provided by DWM
The Designated Person for Safeguarding is Mrs Kerry Young (Shillington) and Miss Sarah Woodham (Stondon)

Monitoring and Evaluation

This policy will be reviewed by the Full Governing Body every three years.

Links to Other Policies

Safeguarding Policy
Promoting Positive Behaviour Policy
Acceptable Use of ICT Policy
Home – School Agreement