Silverhill Primary School
Policy for Digital-Safety

Safeguarding	Issue date; Jan 2018	Review date;April 2020

The Digital-Safety Policy is part of the Computing Policy and School Strategic Plan and relates to other policies including those for Computing, Anti-bullying and for Child Protection.

Our Digital-Safety Policy has been written by the Computing Co-ordinators and the Child Protection Officer.

Teaching and learning

Why is Internet use important?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Internet use to enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Filtering is provided though the Lead IT Services.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Evaluation of Internet content

The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils comply with copyright law.

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The evaluation of on-line materials is a part of every subject.

Managing Information Systems

Information systems security

Local Area Network security issues:

- Users must act reasonably – e.g. the downloading of large files during the working day will affect the service that others receive.

- Users must take responsibility for their network use.
- Workstations are secured against user mistakes and deliberate misuse.
- Server is located in Lower Junior Wing
- The server operating system is secured and kept up to date.
- Virus protection and Firewall services for the whole network is installed and updated regularly by LEAD IT.

Wide Area Network (WAN) security issues:

- Personal data will only be sent over the Internet by secured school email addresses.
- Personal carried on portable media will be encrypted or otherwise secured.
- Portable media may not be used by pupils without specific permission followed by a virus check. Staff may use portable media. They must be encrypted.
- Unapproved system utilities and executable files will not be allowed in pupil's work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.
- The Computing co-ordinators will review system capacity regularly.

Management of e-mail

Staff are provided with e-mail accounts though the Lead IT. Staff e-mail addresses take the form firstname.surname@silverhill.derby.sch.uk. Pupil's e-mail accounts are in a walled garden and default to being able to send within school only. Wider access can be arranged for e-mail use for specific educational projects. Pupils are encouraged to access their e-mail accounts through the Learning Platform.

- Pupils may only use approved e-mail accounts provided through the Virtual Learning Environment (VLE)
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to external organisations 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.

Text messaging

Parents are contacted using Teachers2Parents.co.uk. Mobile numbers are online and protected by a SSL 128 bit certificate. This is the same protection technology used by online banking. All of their staff are DBS checked and the company is fully registered with the data protection register.

New parents will be asked for their details when their child starts school. Any undelivered messages will be followed, up as this may mean incorrect numbers or full mailboxes.

Management of published content

The school has a website. The contact details on the website are the school address, admin e-mail and telephone number. Staff or pupils' personal information is not published. The website coordinator, school business manager and Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publication of pupil's images or work

- Staff will ensure that only digital cameras provided by the school will be used to photograph pupils. Staff should not use personal mobile phones to take photographs of children, except with the specific approval of the Headteacher.
- Staff will ensure that all photographs of pupils are deleted from the school digital cameras as soon as practically possible once transferred.

- Staff will ensure that no photograph or image of pupils will be transferred to personal or home computer systems this also includes personal USB devices.
- The school operates an 'opt out' policy for photograph permissions. Pupil's photographs may be published on the school website, blog and twitter feed unless parents have opted out upon admission to school.
- Pupils' full names will not be used anywhere on the school web site or other unsecured on-line space.
- Work can only be published with the permission of the pupil and parents/carers.
- Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories upon admission to school.

Management of social networking and personal publishing

- The schools will block access to social networking sites.
- Pupils will be given opportunities to use the social networking tools available through the 'Switched On Computing' scheme of work to enable them to experience social networking in a secure environment.
- 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 and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph, which could identify the student or his/her location e.g. house number, street name or school.
- Staff should not accept minors as 'friends' on social networking sites.
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils are encouraged to invite known friends only and deny access to others.
- Pupils are advised not to publish specific and detailed private thoughts.
- Pupils are advised not to engage in voice chat with anyone whom they do not know personally.
- The school is aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

Management of filtering

Internet filtering is provided by LEAD

If staff or pupils discover unsuitable sites, the URL must be reported to LEAD Ltd via email. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

Management of Videoconferencing

The Equipment and Network

- Videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses should not be made available to other sites.
- Videoconferencing contact information is not put on the school Website.

Users

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.

- Videoconferencing should be supervised appropriately for the pupils' age.
- Parents and guardians should agree for their children to take part in videoconferences.
- Only key administrators should be given access to the videoconferencing system, web or other remote control page available on larger systems.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Content

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference.
- If third-party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class.

How can emerging technologies be managed?

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- Pupil mobile phones are not allowed in school. Permission must be sought from the head teacher if parents deem it necessary for health and safety reasons. On such occasions mobile phones should be handed in and collected from the school office.
- The school will investigate wireless, infra-red and Bluetooth communication technologies.
- Staff have access to a school phone and messaging service where contact with pupils is required.

How should personal data be protected?

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. The school has a Data Protection Policy in place.

Risk assessment

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor DCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will review Computing use to establish if the Digital-Safety policy is adequate and that the implementation of the Digital-Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Digital-Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Pupils and parents will be informed of the complaints procedure. A copy of which is on the website.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Discussions will be held with the Derby Safeguarding Children's Board (DSCB) to establish procedures for handling potentially illegal issues.
- Sanctions within the school discipline policy include:
    - Interview/counselling by senior member of staff
    - Informing parents or carers
    - Removal of Internet or computer access for a period.

Communicating the Policy

Introducing the policy to pupils

- Pupils will be informed that network and Internet use will be monitored.
- A Digital-Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use should precede Internet access.
- An Digital-Safety module is included in every unit of the 'Switched On Computing' scheme of work that the school have adopted, and will cover the use of technologies safely when both in school and at home
- Regular whole assemblies are held by the Computing coordinators to highlight the importance of Digital-Safety and the latest risks.
- Failure to adhere to the policy will result in the pupil's access to the internet/computing resources being removed.
- An annual 'Digital-Safety' day will be held in all classes across KS1 and KS2.

Introducing the policy with staff

- All staff in school will be given the School Digital-Safety Policy and its application and importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Training in safe and responsible Internet use and on the school Digital-Safety Policy will be provided as required.

Parents' support

- Parents' attention will be drawn to the school's Digital-Safety Policy in newsletters, the school brochure and on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.