Silverhill School

8.02

Internet Policy

- This policy applies to both on and off-site activity.
- All staff and pupils will be granted internet access.
- Please also refer to 'Staff Acceptable Use of ICT Policy', Policy for Security of Confidential Information on Portable Media, Policy on the Safe Use of Images and 'Tapestry Policy'
- Silverhill School subscribes to IT support services hereafter referred to as 'IT support'.
- For service provider details please contact the school office.

Why have an internet policy?

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource for all to use on a daily basis. However, some of the material is published for adult audiences and is unsuitable for children. Sadly email and chat communication can also be used inappropriately and therefore it is a necessity to provide our children with protection from inappropriate material or communications.

The importance of the internet in school

The purpose of using the Internet 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, information and business administration systems.

Using the Internet is part of the statutory curriculum and a necessary tool for staff and children. The Internet has enormous potential to enhance the learning process. In the world of education, the development of the Internet is the most significant advance in technology since the invention of printing. Its potential to unlock new ways of teaching and learning is immeasurable.

How the internet benefits education

Benefits of using the Internet in education include:

- Inclusion in government initiatives such as the South West Grid
- Professional development for staff through access to national developments, educational materials and good curriculum practice
- Communications with support services, professional associations and colleagues within and outside the county/borough

- Exchange of curriculum and administration data with the local education authority (LA) and Department for Education (DfE)
- Improved access to technical support including remote management of networks
- Access to worldwide educational resources including museums and art galleries
- Educational and cultural exchanges between email worldwide.
- Raising standards by giving access to knowledge beyond that which is immediately available in the classroom.

Ensuring internet access is appropriate and safe

Children in school are unlikely to see inappropriate content in books because publishers, teachers and other education staff select books carefully. Similarly, we take the following key measures to help ensure that our children are not exposed to unsuitable material via the Internet:

- Our Internet access is monitored and maintained by IT support who provide a filtering system
- Children using the Internet are normally working in classes, during lesson time, and are supervised by an adult (usually the teacher) at all times
- Staff check that the pre-selected websites for use by the children are appropriate to their age and maturity
- Staff are particularly vigilant when children are undertaking their own searches and check that they are searching responsibly
- Children are taught to use email and the Internet responsibly, in order to reduce the risk to themselves and others
- The ICT co-ordinator monitors the effectiveness of Internet access strategies
- The ICT co-ordinator ensures that occasional checks are made on files to monitor compliance with the school's policy
- The Headmistress ensures that the policy is implemented effectively and this is monitored by the school's Child Protection Officer
- Methods to quantify and minimise the risk of children being exposed to inappropriate material including on-line grooming and radicalisation are reviewed in consultation with colleagues from other schools and advice from the LA, our IT support company and the DfE.
- Staff are vigilant about the content of email **(See Email Best Practice Guidelines)** and web pages
- Staff will ensure children are aware of the e-safety guidelines and follow the advice provided on www.kidsmart.org.uk

Introducing the policy to pupils

- Rules for Internet access will be posted in all rooms where computers are used
- A module on responsible Internet use and e-safety will be included in the curriculum covering both school and home use. This will include the necessity of keeping personal information safe, how to use mobile technologies appropriately and using online communication appropriately.
- Instruction on responsible and safe use should precede Internet access
- Pupils will be informed that Internet use will be monitored

Parents and E-Safety

- Information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.

What happens if children encounter inappropriate material?

Despite these precautions, the scale of the Internet, that it is international and that much of the material is linked mean that it is not possible to *guarantee* that any particular type of material will never appear on a computer screen. *The school cannot accept liability for the material access, or any consequences thereof.*

- Children are taught to tell a teacher **immediately** if they encounter any material that makes them feel uncomfortable or is inappropriate.
- If there is an incident in which a pupil is exposed to offensive or upsetting material the school will respond to the situation quickly and on a number of levels.
- Responsibility for handling incidents involving children will be taken by the responsible adult (usually the class teacher), the ICT Co-ordinator and the Headmistress.
- All teaching staff will be made aware of the incident at a Staff Meeting if appropriate. In all circumstances a report will be logged by the class teacher and passed on to the School Office who will report this to IT support.
- If one or more children discover (and /or view) inappropriate material, our first priority will be to give them appropriate support. The child's parents/carers will be informed and given an explanation of the course of action the school has taken. The school aims to work with parents/carers and children to resolve any issues.
- If any staff or pupil discovers unsuitable sites, IT support, via the School Office, will be informed. The member of staff on duty will report the web address and its content to IT support and to the LA where appropriate. The site will be blocked.
- Children are expected to play their part in reducing the risk of viewing inappropriate material by obeying the *Rules of Responsible Internet Use* **Appendix 1**.
- Children who abuse the privileges of Internet and email access by failing to follow the rules they have been taught or failing to follow the agreed search plan will have sanctions applied.

Maintaining the security of the school's ICT network

Connection to the Internet significantly increases the risk that any computer or network is infected by a virus or accessed by unauthorised persons.

- The school's IT provider subscribes to antivirus protection where an up-to-date scan takes place to ensure system security from latest viruses or any information that may harm our network.
- An **automatic shut-down** system is used to help maintain security – see **Appendix 2**

Using the internet to enhance learning

Children learn how to:

- use web browsers
- use search engines
- find and evaluate information via the Internet

Access to the Internet is part of planned curriculum time that enriches and extends the learning activities integrated into our schemes of work.

As in other areas of work, we recognise that children learn most effectively when given clear objectives. Internet access is designed expressly for pupil use and includes a filtering service provided by IT support. Children use different ways of accessing the Internet depending upon their age and the nature of material required:

- Children will not be issued individual email accounts unless monitored accounts, but will be authorised to use a group/class email address under supervision if necessary.
- At Key Stage 1 access to the internet will be by adult demonstration with directly supervised access to specific, approved online material.
- Access to the Internet may be demonstrated by the teacher (or sometimes other adult)
- Children may access teacher-prepared materials, rather than the 'open Internet'
- Children may be directed to a specific web page or website to use
- Children may be provided with a list of relevant and suitable sites which they may access
- The school will work in partnership with parents and our IT support team to ensure systems to protect pupils are regularly reviewed and improved
- Methods to identify, assess and minimise risks will be reviewed regularly
- Older, more experienced children may be allowed to undertake their own Internet search having agreed a search plan with their teacher. Children will be expected to observe the *Rules of Responsible Internet Use* and will be informed that checks can and will be made on files held on the system and the sites accessed.

Children accessing the Internet will be supervised by an adult, normally their teacher, at all times. They will only be allowed to use the Internet once they have been taught the *Rules of Responsible Internet Use* and the reasons for these rules. Teachers will endeavour to ensure that these rules remain uppermost in the children' minds as they monitor the use of the Internet.

Using information from the internet

To use information from the Internet effectively, it is important for children to develop an understanding of the nature of the Internet and the information available on it. In particular, they should know that, unlike the school library, for example, most of the information on the Internet is intended for an adult audience, much of it is not properly audited/edited and most of it is copyright.

Therefore:

- Children are taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV
- Teachers will ensure that children are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the Internet
- When copying materials from the web, children are taught to observe copyright laws
- Children are made aware that the writer of an email or an author of a web page may not be the person claimed

In addition:

- Children will not be permitted access to any public or un-moderated chat rooms for any reason.
- Pupils will learn appropriate Internet use and be 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.

On-line communications and social networking

- Safe use of the internet and specifically Social Network sites will be taught as part of the computing curriculum
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils
- Pupils will be advised to use nicknames and avatars when using social networking sites as part of the e-safety programme
- Staff development in safe and responsible Internet use and on the school Internet policy will be provided as required

Silverhill school website

- Our school website is intended to provide accurate, up to date information about our school.
- The School Office is responsible for ensuring that pages are up-loaded to the school site regularly, that the links work and that the site meets the requirements of the host.
- The point of contact on the website is the school's address, telephone number and email address.
- We do not publish children's full names or children's photographs accompanied by names that identify individuals on our web pages.
- Home information or personal email addresses will not be available either.
- Photographs of pupils will not be published on the school website/social media page when parents/carers have expressed this preference.

- Where audio and video are included (podcasts/video blogging) the nature of the items uploaded will not include content that allows pupils to be identified.
- A list is prepared by the Front Office of pupils whose parents do not wish for their images and recordings to be used on the internet.
- School staff are responsible for ensuring they check this list for any restrictions as per above.

Our school website can be found at: www.silverhillschool.co.uk

E-safety using portable equipment

- The school does not permit children to bring their own electronic equipment into school (e.g. includes digital cameras, MP3 players) unless agreed and authorised by a member of staff. The exception is an e-reader (e.g. Kindle).
- Any such items must be clearly labelled and are brought in at their own risk.
- Staff are required to ensure that any portable equipment they may bring into school – PDAs, mobile phones, laptops, music players etc. are kept secure and that children cannot access them.
- Any such item found with inappropriate material will invoke disciplinary measures (see Policies and Procedures for Staff Conduct).
- There may be occasions when children are issued with portable electronic equipment by the school for certain projects and exercises e.g. tablets, digital cameras, video cameras, dictaphones. Where possible, the use of this equipment will be supervised by a member of staff, however all children will be taught the correct, safe and appropriate use of such equipment and made aware what is deemed to be inappropriate and the consequences.

Remote access to the school network

- The School network can be accessed remotely by authorised users only.
- Approved users will have access to the appropriate resources according to the level of access permission granted.
- School files should not be saved on any devices which are not school computers unless prior permission has been given by the Headmistress.
- School data including confidential data must not be stored or taken off the school premises on any portable device without express permission of the Headmistress and then only if it is encrypted.
- Access by unauthorized persons to the schools network is an offence and may result in prosecution under the Computer Misuse Act 1990.
- The school data will conform to the requirements of GDPR and Data Protection Act 2018.

Breach of policy

If an adult breaches school policy, concerns will be taken seriously, logged and investigated appropriately.
If inappropriate material is found on school property, Child Protection procedures will be initiated.

Children Using Email

Children learn how to use an email application and are taught email conventions. Children will have a class-based email address and from Year 3 will begin to use email to communicate with others, to request information and to share information.

It is important that communications with persons and organisations are properly managed to ensure appropriate educational use and that the good name of the school is maintained.

Therefore:

- Children are only allowed to use email once they have been taught the Rules of Responsible Internet Use and the reasons for these rules
- Teachers endeavour to ensure that these rules remain uppermost in their minds as they monitor children using email
- Children may send emails as part of a planned lesson through a class email address that the teacher has authority over, but will not be given individual email accounts
- Incoming email to children is not regarded as private and may be opened and read by the class teacher before allowing pupil access
- Children have their outgoing email messages checked by a member of staff before sending them
- The forwarding of chain letters is not permitted
- Children are not permitted to use email at school to arrange to meet someone outside school hours

Related Policies:

- Anti-bullying Policy – regarding the school's policy on handling cyber-bullying

See Appendix 1 – Rules for Responsible Internet Use

Web Based Resources

For Schools

KidSmarthttp: www.kidsmart.org.uk
SMART rules from Childnet International and Know It All for Parents

Childnet International http://www.childnet-int.org
Guidance for parents, schools and pupils

Bectahttp: www.schools.becta.org.uk/index.php?section=is - e-Safety Advice

Becta / Grid Club, Internet Proficiency Scheme.
On-line activities for Key Stage 2 pupils to teach e-safety
http://www.gridclub.com/teachers/t_internet_safety.html

South West Grid for Learning http: www.swgfl.org.uk/onlinesafety

DfE Anti-Bullying Advice http: www.gov.uk/governmnet/publications/preventing-andtackling-bullying

Grid Club http://www.gridclub.com/teachers/t_internet_safety.html

Internet Watch Foundation www.iwf.org.uk - Invites users to report illegal Websites

South West Grid for Learning – Safe www.swgfl.org.uk/safe
A comprehensive overview of web-based resources to support schools, parents and pupils

Think U Know www.thinkuknow.co.uk/
Home Office site for pupils and parents explaining Internet dangers and how to stay in control.

For Parents

Kids Smart http://www.kidsmart.org.uk/parents/advice.aspx
A downloadable PowerPoint presentation for parents

Childnet International http://www.childnet-int.org/

"Know It All" CD-ROM free to order resource for parents to help raise awareness of how to help their children stay safe online.

Legal frameworks

- **Computer Misuse Act 1990** makes it a criminal offence to gain access to a computer without permission. The motivation could be technical challenge, data theft or to damage the system or data.
- **Monitoring** of data on a school network could contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the rights for private and family life, which is protected by the Human Rights Act 1998. The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 also limit monitoring. The 2000 Regulations apply to all forms of electronic monitoring and interception irrespective of whether the material monitored is generated by private use or in the course of the school's day-to-day activities.
- **GDPR & Data Protection Act 2018** concerns data on individual people held on computer files and its use and protection.
- **Copyright, Design and Patents Act 1988** makes it an offence to use unlicensed software
- **Telecommunications Act 1984** Section 43 makes it an offence to send offensive or indecent materials over the public telecommunications system
- **Protection of Email Act 1978**
- **Obscene Publications Act 1959 and 1964** defines "obscene" and related offences

This policy was adopted by	Silverhill School and Day Nursery
Date	January 2019
Review Date	January 2020
Name of signatory	Jenifer Capper
Role of signatory	Headmistress

APPENDIX 1

Rules for Responsible Internet Use

The school has installed computers with internet access to help our learning. These rules will help keep us safe and help us be fair to others.

Using the computers:

- I will only access the computer system with the login and password I have been given
- I will not access other people's files
- I will only work at my own station and not interfere with the work of others
- I will not bring in memory sticks or CDs from outside school and try to use them on the school computers unless I have permission from a teacher

Using the internet:

- I will ask permission from a teacher before using the internet
- I will report any unpleasant material to my teacher immediately because this will help protect other pupils and myself
- If I accidentally find anything unpleasant or nasty, I will turn off my **monitor** and tell my teacher immediately
- I understand that the school may check my computer files and may monitor the internet sites I visit
- I will not complete and send forms without permission from my teacher
- I will not give my full name, my home address or telephone number when completing forms
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- I understand that if I deliberately break these rules, I may not be allowed to use the internet or computers

Child's Name…… Year Group……..

Signature…… Date……..

APPENDIX 2

Automatic Shutdown

After being first turned on in the morning, all PC's should be left on throughout the day.

Your computer will be automatically shut down every evening.

The benefits of doing this include:

- Safety - ensuring computers are not left in 'sleep mode' overnight means less chance of electrical fires.
- Security - if a machine is switched off it cannot be infected with viruses or be hacked.
- Power saving - a switched off machine will use very little power - saving energy, money and the environment.
- Updates - updates happen regularly and the majority are applied when you start your machine up. Regularly shutting down your machine ensures that it is fully up to date.
- Minimising damage – a computer that is incorrectly turned off can damage the hard drive.

How it works

All users should ensure that all data is saved and files are closed before shut down.

- Shut-down commences automatically at 18:00 every evening
- There is a 10-minute countdown (from 18:00) to allow anyone who is logged on to save their work.
- You will need to save your work before the shutdown starts otherwise you will lose it.
- Any machine can be switched on again after it has been shut down, if so required.
- The process is repeated Saturday and Sunday evenings to capture any weekend use.

IT suite computers

It is recommended that the computers in the IT suite are switched on first thing in the morning and before the class begins.

If it takes more than 5 minutes to power up your machine when you switch it on again in the morning, please contact the School Office and fill out an IT Help Request form.

Small changes to make a big difference

In the IT Suite in particular there has been a high incidence of failed hard drives which could be due to a problem with computers being left on over-night and incorrectly shut down in the morning. By shutting down the computers overnight there will be savings in energy costs as well as a carbon reduction and the frustrations of inoperable computers is reduced.