Responsible use of ICT Policy

Scope of the Policy

This policy applies to all members of the Sunningdale School Community (including Governors, staff, students / pupils, volunteers, parents / carers, visitors who have access to and are users of Sunningdale ICT systems, both in and outside the school premises.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within Sunningdale School.

Governors

The Governors are responsible for the approval of the *IT & Online Safety Policy* and for reviewing the effectiveness of the policy. Governors will review effectiveness by receiving regular information about online safety incidents and monitoring reports from senior leaders.

Headteacher and Senior Leaders

The Head Teacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety in conjunction with the IT Team.
The Head 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 online safety allegation being made against a member of staff. See the Dealing with Allegations of Abuse against staff guidelines.
The HT will receive regular reports on matters of online safety

Technical staff

The ICT Team is responsible for ensuring:

- that the Trust's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements.
- that users may only access the networks and devices through an appropriate password protection policy
- the filtering policy, is applied and updated on a regular basis appropriate for each school
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as

relevant

- that the use of the network, internet, Learning Platform, remote access, email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher or Head of School for investigation / action / sanction

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current Sunningdale School IT and Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher.
- all digital communications with students / pupils / parents / carers should be on a professional level *and only carried out using official school systems*.
- online safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the IT & Online Safety Policy guidelines as appropriate
- the whole school community have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- Whenever the internet is used pupils should be guided to sites suitable for their use and that processes are in place for dealing with any unsuitable material from internet searches.

Designated Safeguarding Lead

Should be trained in online 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

- be guided by staff in using technology safely and appropriately
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good online safety practice when using digital technologies out of 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' evenings, newsletters, letters, website and information about national and local e

safety campaigns or 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
access to parents' sections of the website/social media accounts/on-line learning observations.

Why is Internet use important?

The purpose of Internet access in schools 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. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet access is an entitlement for pupils who show a mature and responsible approach to its use. The Internet is an essential element in 21st century life for education, business and social interaction. Our school has a duty to provide pupils with quality Internet access as part of their learning experience.

How does the Internet benefit education?

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and galleries.
- Inclusion in Government initiatives such as the DCFS ICT in Schools and the Virtual Teacher Centre (VTC).
- Education and cultural exchange between pupils worldwide.
- Immediate access to up to the minute news and current events.
- Cultural, vocational, social and leisure use in libraries, clubs and at home.
- The opportunity for staff and pupils to discuss with experts in a variety of fields.
- Staff professional development through access to national developments, educational resources and good curriculum practice.
- Communication with support agencies, professional associations and colleagues.
- Improved access to technical support including remote management of networks.
- Exchange of curriculum and administrative data with LA and DCFS Scope

This policy applies to all school equipment at any time including any laptops signed out by staff for use at home. Visitors should seek the Headteacher's permission before bringing their own equipment onto the premises.

Risk Assessment

As with a number of other media sources, such as magazines, books and videos, the Internet contains material unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material by using Sunderland's filtering system and children will not be allowed Internet access without the presence of an adult member of staff. Staff supervision is paramount in taking all reasonable precautions to ensure only appropriate material is accessed.
However, even with adult supervision, it is impossible to guarantee that particular types of material will never appear on a computer terminal or

station. This is due to the international scale and linked nature of material on the Internet. Neither the school nor Sunderland LA can accept liability for inadvertent access to material accessed or to the consequences of such access. 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 annually. The Headteacher will ensure that the Internet policy is implemented and compliance with the policy monitored.

Policy Decisions

- No pupil will use the ICT without adult supervision.
- Pupils must have permission to use the Internet.
- Pupils may work independently when directed to a website which has already been vetted by the teacher.
- Free searching (use of general search engines) is forbidden to children except recommended children's search engines such as yahooligans or ask kids, when they will be supervised.
- Only an adult or children under supervision will do the downloading of files or images.
- Children will not use or be issued with individual e-mail accounts (adult staff may set up and use their own account). They must only use approved email accounts set up on the school system.
- Sent messages will be moderated by the teacher and must be polite, appropriate and justified.
- Pupils must not reveal personal details of themselves (home address, telephone number) or others in e-mail communication, or arrange to meet anyone.
- Pupils must immediately tell staff if they receive an offensive email.
- E-mail sent to external organisations must be authorised before sending, in the same way as a letter written on school headed paper.

Social networking and personal publishing

- The school blocks access to social networking sites
- Newsgroups are also blocked
- Pupils are told never to give out personal details which may identify them
- Pupils and parents are advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Authorising Internet Access

- The school agrees to Internet access based on educational or professional development needs without prior permission.
- Other reasonable use of the Internet may be allowed but must be agreed to by school leaders before use.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff or pupil may leave or a pupil's access be withdrawn. There will be a separate access for students and supply staff.
- At Key Stage 1 Internet access will only be through adult or teacher demonstration. Children may access teacher prepared files or materials rather than open the Internet.
- At Key Stage 2 Internet access will be granted to the whole class based on a lesson need that corresponds to the ICT or cross curricular Schemes of Work. Children must first have been given a suitable introduction to rules for responsible use of the Internet.

- Pupils will be allowed supervised use of the Internet for research or reference outside of class time (e.g. break times or after school clubs)

Maintaining a Secure Computer System

- The school's internal network is secure via a firewall. It is maintained by the school's external IT Provider.
- Virus protection software is installed and is updated as is reasonably practicable.
- The use of CD-ROMS and memory USB sticks by children is forbidden. Staff may use them vigilantly, reporting screen displays immediately. Staff should also be mindful of viruses when using memory sticks between machines.
- The external IT Team will ensure system capacity is reviewed to take the ever-increasing use of the Internet.
- Children's work is subject to monitor at anytime by the child's class teacher or a senior leader.
- Children may store any saved files within their allocated drive and folder.
- Files not attributed to allocated areas are subject to immediate deletion.
- Data Protection
- Staff must only use encrypted memory sticks.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Procedures for Reporting Inappropriate use of I.T.

- Responsibility for handling incidents will be delegated to the HT or senior leader.
- The supervising adult must turn off the monitor but not the base unit.
- A message needs to be forwarded to a senior leader.
- The SL will privately review the nature of the material and log the terminal number/location, the date, time and nature of material found, who found it and the user login if appropriate.
- Any complaint about staff misuse must be referred to the Headteacher.

Staff Use of computers/lap tops

The Internet on school computers should not be used for any political purposes, personal gain or social use e.g. personal emails, booking holidays, private financial matters or social networking.

- School computers and lap tops should only be used for professional purposes.
- Inappropriate use of the Internet will be subject to disciplinary action.

Keeping staff and pupils aware of their Conditions of Use

All staff and adults working in school will be given a copy of the 'Acceptable and Responsible Use of Internet Policy' and its importance explained. If they feel unprepared for Internet use then the ICT co-ordinator will spend time tutoring the basics to them. Reassurance and discussion are always available from the ICT coordinator.

Parental Support

Parents' attention will be drawn to the Acceptable and Responsible Internet Use document in newsletters and the school website. Internet issues will be handled sensitively to inform parents without undue alarm. A partnership approach with parents will be encouraged. Home use is increasing at possibly

a faster rate than school use and parents must be made aware/reminded of the dangers of unrestricted access. Supervised use of the Internet at home is encouraged. The school is available to discuss any issues/concerns about the Internet or other IT use.
Interested parents will be referred to organisations such as PIN (Parents Information Network), Parents Online and National Action for Children.

Review

The Governing body will review this policy every annually. The Governors may, however, review the policy earlier than this if the government introduces new legislation, or if the Governing Body receives recommendations on how the policy may be improved.