Sir John Nelthorpe School

Online Safety Policy

Author	Mr S Howe
Last reviewed	Spring Term 2019
Next review date	Spring Term 2020
Consultations / Training	Governors

Introduction

This policy for all staff, governors, students and guests, is implemented to protect the interests and safety of the whole school community.

The school encourages students to make use of the information resources available on the Internet, together with the development of appropriate skills to analyse and evaluate such resources. These skills will be fundamental in the society our students will be entering.

On-line services significantly alter the information landscape for schools by opening classrooms to a broader array of resources. In the past, teaching and library material could usually be carefully chosen. All such material would be chosen to be consistent with national policies, supporting and enriching the curriculum while taking into account the varied teaching needs, learning styles, abilities and developmental levels of the students.

Internet access, because it may lead to any publicly available site in the world, will open classrooms to electronic information resources which have not been selected by teachers as appropriate for use by students. So therefore unfettered access needs to be controlled.

The school expects that staff will blend use of such information as appropriate within the curriculum and that staff will provide guidance and instruction to students in the appropriate use of such resources.

The school believes that the advantages students gain from access if online to information resources and the increased opportunities for collaboration exceed the disadvantages. Ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the school supports and respects each family's right to decide whether or not to apply for independent access for their child.

Roles and responsibilities

The Designated Safeguarding Lead, ICT subject lead and IT Support have responsibility for ensuring this policy is upheld by all members of the School Community and updated annually or when there is a concern, whichever is sooner. They will keep up to date on current online safety issues and guidance issued by organisations such as the Local Authority and CEOP. As with all issues of safety at this school, staff are encouraged to create a talking culture in order to address any online safety issues which may arise in classrooms on a daily basis.

Online safety in the curriculum and school community

The School provides opportunities to teach about online safety within a range of curriculum areas including ICT. Educating students on the dangers of technologies that may be encountered outside school will also be carried out via ICT, PSHCE, assemblies, tutor time, displays and informally when opportunities arise.

At age-appropriate levels students are taught to look after their own online safety, this includes: respecting other people's information and images, recognizing online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across.

Use of the internet to enhance learning

- The school internet access will be designed expressly for student use and will include filtering appropriate to the age of students.
- On entry to the school, ICT lessons will teach students what internet use is acceptable and what is not. Across the curriculum staff will guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- If staff discover unsuitable sites, the URL (address) and content must be reported to IT Support
- The use of internet derived materials by staff and students will comply with copyright law with acknowledgement of sources as appropriate.

Authorisation of internet access

- A record of all students and staff who have been granted internet access will be held by the school and kept up-to-date
- Students will be informed that internet use is monitored and breaches of online safety will be recorded and dealt with under the 'Rewards and Sanctions' policy.

Risk Assessment

- In common with other media some material via the internet is unsuitable for school students. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the *Computer Misuse Act 1990.*
- Access to websites that involve gambling, games (unless educationally relevant) or financial scams is strictly forbidden.
- The use of school equipment for file sharing copyrighted material is forbidden.
- Strategies to identify, assess and minimise risks will be reviewed regularly.

Managing filtering

- The school will work in partnership with parents; the LA, DFE and the Internet Service Provider to ensure systems to protect students are reviewed and improved.
- The Internet Gateway will be managed, maintained and monitored by the Local Authority
- The Headteacher or representative 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 referred to the Internet Watch Foundation (www.iwf.org.uk).
- **In-house filtering will be appropriate to the age and curriculum requirements of the students and used in conjunction with school based 'policies' by which appropriate internet content is identified in advance of curriculum delivery.**

Management of email

- Students may only use approved email accounts on the school system, which they are aware are subject to monitoring.
- Access in school to students' personal e-mail accounts will be blocked.

- The forwarding of chain emails is prohibited.
- If a student receives offensive email, it must be reported immediately to a teacher, who may require it forwarding to an appropriate work email account to assist with further investigation.
- Students must not reveal details of themselves or others in email communication or via personal web space, such as address or telephone number, or make arrangements to meet anyone
- E-mail sent to an external organisation by a student must be authorised by a teacher before sending.
- Inappropriate personal email or messaging between staff and students/students is not permitted.

Managing website content

- The point of contact on the website will be the school address, school email, fax and telephone number
- Photographs of students on the website will be carefully selected, students' names will not be used with photographs or articles
- On an annual basis the school will seek permission of parents' and carers regarding the use of student photos in any publication
- The Headteacher or representatives will take overall responsibility for the accuracy and appropriateness of content
- The copyright of all material is held by the school, or attributed to the owner where permission to use material has been obtained

Newsgroups E-mail lists and forums

- Interest groups and forums will only be made available to students through the schools learning Platform (0365). Access to forums that are moderated by a responsible person or organisation and are directly linked to an educational activity will be permitted.

Chat, Instant messaging, Blogs and social networking sites

- Students will not be allowed access to public or unregulated chat rooms or social networking sites
- Permission may be granted by the Headteacher or representative to access regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised as part of the learning objective.
- A risk assessment will be carried out before students are allowed to use a new technology in school.
- Staff must ensure that social networking sites are set to 'private' preventing access from students.
- Staff must not to be 'friends' with any student on a social networking site. E.g. Facebook, Myspace and twitter.
- If a student has attempted to initiate an online communication through a social networking site or other online facility, the member of staff should record this and decline the invitation. Repeated attempted contacts should be logged and the line manager informed.

Personal websites

- When publishing material to websites and elsewhere, students should consider the thoughts and feelings of those who might view the material. Material that victimises or

bullies someone else, or is otherwise offensive, is unacceptable and may also be illegal.
- Should a member of staff design a website there must not be mention, either directly or otherwise, of Sir John Nelthorpe School or persons within the organisation.

Photographic, video and audio technology

- When not in use, video conferencing cameras should be switched off and turned to face a wall.
- Care should be taken when capturing photographs or video to ensure that all students and staff are appropriately dressed. It is not appropriate to use photographic or video devices without direct supervision of a member of staff.
- Staff may use photographic or video devices that belong to the school (including digital cameras and mobile phones) to support school trips and curriculum activities.
- Students must always seek the permission of their teacher before making audio or video recordings for curriculum purposes within school.

Managing emerging ICT applications

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The use of mobile phones by students for any purpose is not permitted during the school day.
- The use of any personal Bluetooth or wireless enabled device is not allowed to by students in school.

Personnel

- All staff have a responsibility for **ONLINE SAFETY.**
- All new staff will be asked to confirm they have read this policy as part of their induction. Copies of the policy are available in the policies area of the school network
- Staff should be aware that internet traffic is monitored and can be traced to the individual user.
- Staff development in safe and responsible internet use will be provided as required
- It is the responsibility of the individual member of staff to ensure that material contained in their files is fit for purpose and does not contain any offensive or copyright material
- Breaching the online safety policy may result in disciplinary action being taken. Access to ICT maybe restricted or removed.

Maintaining the security of the ICT systems

- The school systems will be reviewed regularly with regard to security. Virus protection will be updated regularly
- Files held on the school's network will be checked regularly
- Unapproved system utilities and executable files will not be permitted in students' work areas or attached to email
- The use of mobile storage devices is only permitted for staff if the device is encrypted. In all cases, staff and students should use the cloud based storage facility, 'One Drive' to store work related material. This data should be 'backed up' by use of "One Drive for Business" or storage on the network.
- Staff are expected to check that any files that they propose to use in school are free from virus/spyware/malware

Handling misuse of the internet

- Responsibility for handling incidents will be delegated to a senior member of staff
- The Headteacher and chair of Governors must be kept informed of any complaint regarding misuse by staff
- Students and parents will be informed that sanctions may be used to deal with misuse including, interview with a member of SLT, informing parents or carers and removal of internet or computer access for a period, which could ultimately prevent access to files on the system
- If an instance of severe misuse is suspected the police will be contacted to establish the legal position and discuss strategies, including advice on how best to preserve any possible evidence

Parental Support

- A partnership approach with parents will be encouraged, including sessions on suggestions for safe internet usage and the issue of guidance leaflets
- Parents' attention will be drawn to the Acceptable Use policy in the Student Planner and asked to confirm their support by providing a signature.
- Additional guidance for parents will be provided via the school website. Parents may also be referred to organisations such as Child Exploitation and Online protection (CEOP). Advice given by the school will be limited to e-safety and will not extend to technical advice
- Internet issues will be handled sensitively to inform parents without causing undue alarm
- The School website has an area dedicated to E-safety and staff, students and parents should check then periodically

Monitoring and review

- Records of student and staff breaches of the policy will be kept in the individual's file. The number and nature of breaches will inform the review of the policy.
- All records relating to breaches of the policy may be shared with legitimate agencies as necessary to ensure e-safety
- The governing body has a responsibility to monitor the effectiveness of the policy and to contribute to policy review

The misuse of internet access and e-technology is a serious matter and appropriate sanctions (including the use of temporary and permanent exclusion) will be used. Staff may also be subject to disciplinary action including dismissal.

Relationship with other Policies

Behaviour, rewards and sanctions policy
Curriculum policy
Staff code of conduct