SEDBERGH INTERNATIONAL

SUMMER SCHOOL

E-Safety Policy

Version	2020.2
Effective from	October 2020
Extent of policy	Sedbergh International Summer School
Policy owner	Gemma Newton
Review by	September 2021
Frequency	Annual
Circulation	Staff and Student Induction; Parents (by request)
Publication	Website

Policy on E-SAFETY

Please refer also to the ISS ICT Acceptable Use Policy.

The Internet is an essential element for education, business and social interaction. Sedbergh International Summer School ("the Summer School") has a duty to provide students with quality Internet access as part of their learning experience.

Pupils use the Internet widely outside of the Summer School and will need to learn how to evaluate Internet information and to take care of their own safety and security.

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The Summer 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 Summer School computer. The Summer 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.*

Methods to identify, assess and minimise risks will be reviewed regularly.

The Course Director will ensure that the E-Safety Policy is implemented and compliance with the policy monitored.

Internet content
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the Internet Service Provider via the IT Department.
- The evaluation of on-line materials is the responsibility of all staff.

ICT system security
- The security of the Summer School ICT systems will be reviewed regularly.
- Virus protection and other security measures will be installed and updated regularly.
- The Summer School will work constantly to ensure systems to protect pupils are reviewed and improved.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the Summer School's network will be regularly checked.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the Summer School is allowed.
- Mobile phones are not permitted in lessons (unless requested by teachers for supervised use in specific lessons) and are collected by House Parents at night to ensure that pupils are not using them at bedtimes.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- The Summer School will keep an up-to-date record of all staff and pupils who are granted Internet access. All internet activity is logged.
- Pupils must apply for Internet access individually by agreeing to comply with the Acceptable Use Policy (AUP).

E-mail management
- Pupils may only use approved e-mail accounts on the Summer School system.
- Pupils must immediately tell a teacher if they receive offensive e-mail e.g. bullying, chain letters, spam etc.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Access in Summer School to external personal e-mail accounts may be blocked.
- Social e-mail use can interfere with learning and may be restricted.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on Summer School headed paper.

Published content
- The contact details on the Website will be the Summer School address, e-mail and telephone number. Pupils' personal information will not be published and staff contact e-mail addresses will only be published in areas restricted to parent access.
- The Course Director or nominee (e.g. Operations Director) will take overall editorial responsibility and ensure that content is accurate and appropriate.

- The Website will comply with the Summer School's guidelines for publications including respect for intellectual property rights and copyright.
- Staff and pupils will be made aware of copyright in respect of material taken from the Internet.

Images or work to be published
- Photographs which include pupils will be selected carefully and will not allow individual pupils to be clearly identified.
- Pupils' full names will not be used in association with photographs anywhere on the Website that is open to the general public, only in the restricted parents' area.
- Parents are asked to 'opt out' of their child being used in school marketing material/ website etc. This option is included within the Summer School's consent form.
- Pupils' work will only be published with the permission of the pupil and parents.
- Use of a mobile device e.g. an iPad, to record still or moving images for publication or to record sound involving pupils, is only permitted when directly related to a curriculum activity or formal assessment and must have the permission of the Course Director.

Social networking and personal publishing education and protection
- The Summer School may block access to social networking sites for all pupils. Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, School, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Students should be encouraged to invite known friends only on to their site and deny access to others.
- Pupils will be advised not to publish specific and detailed private thoughts.
- Pupils will be made aware that bullying can take place through social networking at home especially when a space has been set up without a password and others are invited to see the bully's comments.

E-safety complaints
- Complaints of Internet misuse will be dealt with by the Course Director.
- Any complaint about staff misuse will be referred to the Course Director.
- Pupils and parents will be informed of the complaints procedure.
- Any child protection issues will be referred to the Summer School's Designated Safeguarding Lead (DSL).
- Discussions will be held with the Police liaison officer to establish procedures for handling potentially illegal issues.
- Sanctions within the Summer School discipline policy include: - removal of Internet or computer access for a period of time, detentions and for persistent and/or serious cases, suspension or expulsion will be considered.

Staff

- Staff use of the Internet is permitted and encouraged where such use supports the aims and objectives of the Summer School.
- All staff will be given access to the Summer School E-Safety Policy and its importance explained.
- Staff should be aware that all Internet traffic can be monitored and traced to the individual user and so discretion and professional conduct are essential at all times. The specific content of any transactions will not be monitored unless there is suspicion of improper use. The monitoring of Internet use is a sensitive matter and staff who operate monitoring procedures will be supervised by senior management.
- Should a member of staff breach this protocol, the Bursar has authorised the Course Director to apply the disciplinary procedure which may, in some circumstances, lead to dismissal. Unless negligent under the terms of this protocol, the Summer School accepts no responsibility for any harm caused by a member of staff's use of email and the internet whilst at the Summer School.

Whole staff INSET on safe and responsible use of the internet and on the Summer School's e-Safety Policy will be provided as required.