



INTERNET SAFETY POLICY *(Draft until ratified at next Governor Committee)*

Rationale

Use of the Internet is commonplace and Internet safety depends on staff, schools, governors, advisers and parents to take responsibility for the use of the Internet.

1. Principles for Acceptable Use of the Internet

Use of school computers by pupils must be in support of the aims and objectives of the school and National Curriculum.

Online activities which are encouraged include:

- The use of email and computer conferencing for communication: between colleagues, between pupils(s) and teacher(s), between pupil(s) pupil(s), between schools and industry.
- Use of the Internet to investigate and research curriculum areas.
- The development of pupils' competence in ICT skills and their general research skills.

Online activities which are not permitted include:

- Searching, viewing or retrieving materials that are not related to the aims of the curriculum
- Copying, saving or redistributing copyright-protected material, without approval.
- Subscribing to any services or ordering goods or services, unless specifically approved by the school.
- Playing computer games or using social media sites unless specifically approved by the school.
- Using the network in such a way that use of the network by other users is disrupted (for example: downloading large files during peak usage times; sending mass email messages).
- Publishing, sharing or distributing any personal information about a user (such as: home address; email address; phone number; etc).
- Downloading software.
- Any activity that violates a school rule.

2. Guidelines

Children will:

- Have equal access to email in a safe & secure environment.
- Have equal access to a variety of approved websites through the Intranet.
- Children will be taught all the skills in order to use Internet & email as an ICT tool.
- Children will use Internet & email to support, enhance & develop all aspects of curriculum.
- Children will develop Internet & email skills at the appropriate level regardless of race, gender, intellect and emotional or physical difficulties.
- Children will be reminded of safe searching and laptops, trolleys and classrooms will have posters to remind children of this.
- Children will receive specific Internet Safety skills as part of Child Exploitation and Online Protection Service (CEOPS) and their ICT and PSHE curriculum delivery

Access to the Internet will be withdrawn from students who fail to maintain acceptable standards of use.

Training and staff CPD

External training for pupils and staff is scheduled for every second year to ensure children are safeguarded. Training sessions for parents will also be offered either by school based staff or an external provider. This training will cover all aspects of internet use including social networking sites and the role of CEOPS.

Staff receive on-going training and updates during the cycle of staff meetings. Parents are updated by providing advice via the school website and other means as deemed appropriate. The children learn about E-safety through the curriculum delivered by the teachers and outside visitors.

Appendix A

Guidance on the use of email

Email is still the most common use made of the Internet. This fast and cheap method of communication is available to all staff and pupils. Unfortunately, certain pupils perceive email as a way to send secret offensive messages. Anyone receiving unwanted email should report it immediately to their class teacher or IT co-ordinator. Anyone caught sending such messages should have their access to the technology denied. An email address for the class or in certain instances for groups of pupils makes more sense for certain email-based projects. It also avoids disappointment for individual pupils who do not get replies to their messages.

Guidance for All Users

Staff are encouraged to use ICT resources in their teaching and learning activities, to conduct research, and for contact with others in the education world. Electronic information-handling skills are now fundamental to the preparation of citizens and future employees in the Information Age. Staff are encouraged to investigate the possibilities provided by access to this electronic information and communication resource, and blend its use, as appropriate, within the curriculum. They should model appropriate and effective use, and provide guidance and instruction to pupils in the acceptable use of the Intranet/Internet.

When using the Internet, all users are expected to comply with all laws and government regulations concerning copyright, libel, fraud, discrimination and obscenity and all school staff are expected to communicate in a professional manner consistent with the rules of behaviour governing employees in the education sector.

Pupils are responsible for their good behaviour on the school networks, just as they are on and off school premises. While the use of information and communication technologies is a required aspect of the National Curriculum, access to the Intranet/Internet is a privilege – not a right. It will be given to pupils who act in a considerate and responsible manner, and may be withdrawn if they fail to maintain acceptable standards of use.

Staff should ensure that pupils know and understand that, in addition to the points found under Online activities which are not permitted on page 1 of this document, no Intranet or Internet user is permitted to:

- Retrieve, send, copy or display offensive messages or pictures.
- Use obscene or racist language.
- Harass, insult or attack others.
- Damage computers, computer systems or computer networks.
- Violate copyright laws.
- Use another user's password.
- Trespass in another user's folders, work or files.

Supervising and Monitoring Usage

Teachers should guide pupils toward appropriate materials on the Intranet/Internet. This will avoid a great deal of time wasting as well as going some way towards monitoring the sites accessed by pupils.

Internet access for pupils in schools should be available only on computers that are in highly-used areas of the school such as classrooms and the library. Machines, which are connected to the Intranet/internet, should be in full view of people circulating in the area. Pupils should be supervised when using the Intranet/Internet services.

Teachers and Network administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly. While normal privacy is respected and protected by password controls, as with the Internet itself, users must not expect files stored on the schools intranet or school servers to be absolutely private.

Filtering External Websites

It is an absolute requirement that access to the Internet provided to staff and pupils in any school or educational institution through any Internet Service Provider (ISP) is a blocked or filtered service. Appledore uses South West Grid for Learning which is a blocking service, updated regularly. All users should be aware that the LA can and does track and record the sites visited and the searches made on the Intranet/internet by individual users.

Parents are informed that school provides filtered and monitored access to the Internet for pupils. However, they should also be aware that with these emerging and constantly changing technologies there is no absolute guarantee that a pupil cannot access materials that would be considered unsuitable. The chance of just coming across such materials is highly unlikely, but it obviously increases in direct proportion to the amount of time and effort an individual puts into their search. If you are unfortunate enough to come across any offensive web pages, whilst using school equipment, you are obliged to make a note of the address and report it to the South West Grid For Learning help desk and our technical support specialists.

Google Classroom

- When using Google Classroom and the Gsuite Apps, students will use approved class email accounts under supervision of a teacher or parent/guardian.
- Students will not send or receive any material that is illegal, obscene, defamatory, or that is intended to annoy or intimidate another person.
- Students will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.
- Students will never arrange a face-to-face meeting with someone they only know through emails or the Internet.
- Students will note that sending and receiving email attachments is subject to permission from their teacher.

Distance Learning

In circumstances where teaching cannot be conducted on the school premises, teachers may use Google Classroom, Google Meet, or other platforms approved by school as platforms to assist with remote teaching where necessary.

In the case of Google Classroom and Google Meet, parents/guardians must be required to grant access to their child to have a school Gmail address. Parents/guardians will be provided with the password and will be expected to monitor their child's use of the Gmail address and Online Platforms and agree to monitor their child's participation in any such lessons conducted on the Online Platforms.

Discussion forums on Google Classroom will only be used for educational purposes and will always be supervised.

This policy is reviewed annually.