# Abbey School & EYFS

## E-Safety Policy

**Sylvia Greinig** **September 2019** **Statutory Policy**

# Abbey School & EYFS
# E-Safety Policy

| | |
|---|---|
| Date Policy reviewed | September 2019 |
| Date of next reviewal | September 2020 |
| Reviewed by | SJG and FG |

**Introduction**

The purpose of this policy is to ensure that all staff, parents and children understand and agree the school's approach to e-safety. The policy relates to other policies including ICT curriculum, Internet Access, Bullying, Safeguarding & Child Protection, and Health & Safety.

| | |
|---|---|
| **Designated E-safety Co-ordinator** | **Miss Fleur Greinig (Headteacher)** |
| **E-Safety Lead** | **Mrs Kirsten Gibbs** |

## Teaching and Learning

The purpose of Internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems.

Access to the Internet is a necessary tool for staff and students. It helps to prepare students for their on-going career and personal development needs. It is a requirement of the National Curriculum (NC) for ICT and is implied in other subjects.

### Internet use enhances learning

Internet access is provided by Think IT of Exeter and designed for pupils. This includes filtering appropriate to the content and age of pupils.

Internet access is planned to enrich and extend learning activities.

Access levels are reviewed to reflect the curriculum requirement.

Pupils are given clear objectives for Internet use.

Staff select sites which support the learning outcomes planned for pupils' age and maturity.

Pupils are taught how to take responsibility for their own Internet access.

### Pupils are taught how to evaluate Internet content

Pupils are taught ways to validate information before accepting that it is necessarily accurate.

Pupils are taught to acknowledge the source of information, when using Internet material for their own use.

Pupils are made aware that the writer of an e-mail or the author of a Web page might not be the person claimed.

Pupils are encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

# Managing Internet Access

### Information System Security

School ICT system security is reviewed regularly.
Virus protection is updated regularly.
Security strategies are discussed regularly with ICT advisors.

### E-mail

Pupils do not use email in school.
Pupils must tell an adult immediately if they receive offensive email.
In emails, pupils are taught that they must not reveal their personal details, those of others or arrange to meet anyone without specific permission.
Pupils are taught not to open suspicious incoming email or attachments.
The forwarding of chain letters is not permitted.

### Published content and the school web site

The website complies with the school's guidelines for publications.
Pupils are taught to consider the audience and purpose for the work they publish on the school blog sites and ensure their work is of high quality.
All material must be the author's own work or where permission to reproduce has been obtained, it is clearly marked with the copyright owner's name.
The contact details on the website are for school admin only.

### Publishing pupils' images and work

Photographs must not identify individual pupils.  Group shots or pictures taken "over the shoulder" are used in preference to individual "passport" style images.
Children's photographs are only allowed to go on the website once the child's parents have agreed by signing the appropriate part of the Registration Form.
Children's photographs are not accompanied by names.
Children's names are not accompanied by photographs.
Children's work which contains photographs must not also contain the child's name.

### Social networking and personal publishing

Pupils will not be allowed to access public chat rooms without supervision.
New applications will be thoroughly tested before pupils are given access.

### Managing filtering

The school works in partnership with parents and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

Senior staff ensure that occasional checks are made to ensure that the filtering methods selected are effective in practice. Weekly evidence of this is required to be logged.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT co-ordinator.

### Managing video conferencing and webcam use

Video conferencing is always appropriately supervised.

### Managing emerging technologies

Mobile phones must not be used in school. The sending of abusive or inappropriate text messages is forbidden even from home use.

Cameras in mobile phones are not used by staff or pupils.

Only school cameras are used by both staff and children for educational purposes.

### Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Staff must not keep confidential information on removable devices such as USB devices unless suitably security protected.

## Policy Decisions

### Authorising Internet access

All staff must read the school's "Computers, ICT and acceptable use policy" and the relevant section of the Staff Handbook before using any school ICT source.

The school maintains a record of all staff and children who have access to the school's ICT systems.

Parents are asked to sign a consent form regarding their child's internet use (see Acceptable Use Policy).

Any person not directly employed by the school will be asked to read and sign the "Computers, ICT and acceptable use policy" before being allowed to access the internet from the school site.

### Assessing risks

The school takes all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor Think IT can accept liability for any material accessed, or any consequences of Internet access. The school's e-safety policy and its implementation will be monitored and reviewed on a regular basis.

### Handling e-safety complaints

Complaints of internet misuse must be referred to the ICT Co-ordinator, Miss Greinig.

Any complaint about staff misuse must be referred to the Headteacher.

Complaints of a child protection nature must be dealt with in accordance with the school's child protection policy.

Pupils and parents are informed of the complaints procedure.

Pupils and parents are informed of the consequences for pupil misuse of the Internet (see Computers, ICT and acceptable use policy).

# Communications Policy

### Introducing the e-safety policy to pupils

E-safety posters are posted in the computer suite so that all users can see them.
Pupils are informed that network and Internet use is monitored and appropriately followed up.
The children receive e-safety lessons and are constantly reminded of online safety.

### Staff and the e-safety policy

All staff are trained regularly and receive a copy of the e-safety policy.
Staff are informed that network and Internet traffic can be traced to an individual user.
Staff will always use a child friendly safe search engine when accessing the web with pupils.

### Enlisting parents' and carers' support

Parents’ and carers’ attention is drawn to the school’s E-safety Policy in newsletters and on the school website.
The school has links on its website to e-safety resources.