

BRADDAN SCHOOL

e-Safety Policy

Reviewed April 2022

Next review in line with Policy Review Timeline 2025

Introduction

The DESC requires all schools to have a policy regarding 'e-safety', which details the schools rules and procedures that help to ensure high standards of e-safety for pupils, staff and parents of the school.

This policy should be read in conjunction with the Department of Education, Sport and Culture's acceptable use policy, which all staff and pupils are expected to adhere to.

e-Safety depends on effective practice at a number of levels, and involves close working between the school and DESC ICT division.

Internet Use

Internet use is a part of everyday life for education, business and social interaction. Pupils need to be able to learn how to evaluate internet information and to take care of their own safety and security. The school's internet use is designed to enhance and extend teaching and learning.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for its use.
- Pupils will be taught about the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation of content.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- All pupils will be taught and reminded about e-safety issues as a regular part of the delivery of the ICT curriculum.

Managing Internet Access

Systems in school allow the internet to be accessed from all parts of the school building, and from desktop computers, laptops, and hand held devices such as i-pods and i-pads. Access to these must always be supervised by staff members, and pupils must never have online access that is not directly supervised by an adult.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail (or other online communication), or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Published content and the school website

Pupils are able to access both the student and school wiki's, and leave comments. Pupils will be taught about what constitutes unacceptable comments or remarks as part of the e-safety curriculum. Should inappropriate comments be made, this will be a breach of the acceptable use policy.

- The contact details on the wiki are the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Head teacher and ICT co-ordinator will take overall editorial responsibility and ensure that content is accurate and appropriate.
- All parents must sign a consent form to allow images of their child to be included on the wiki or any website.

Managing filtering

The Department of Education, Sport and Culture operates a web filtering system, but staff must always be vigilant to unsuitable material or sites being accessed, as a great deal of inappropriate content can get through the filtering system. Any instances must be reported to the ICT helpdesk, but pupils themselves must be taught about the meanings and contexts for what constitutes 'acceptable'.

- The school will work with the DESC's ICT support team to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the ICT team leader, (or the Head teacher / Deputy Head teacher), and to the ICT helpdesk.

Social networking and personal publishing

- The school will block/filter access to social networking sites in line with Department policy.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be taught about the potential risks of using social networking sites, in terms of protecting their personal data, and in terms of bullying.

Devices

Pupils are not allowed to bring their mobile phones into school as there is no need for them to have access to these devices during school time. Pupils are not allowed to bring in their other own devices from home, including laptops, gaming devices, i-pods or i-pads, as the school does not deem this necessary in order to enhance or extend pupil learning.

Use of i-pods and i-pads should be clearly linked to objectives for learning in the classroom. Devices may be taken out of class only under supervision of a member of staff.

Pupils will be taught and pupils and staff expected to take appropriate care of all ICT equipment, including replacing items to 'home' bases, plugging in leads, leaving laptop lids open, replacing laptops appropriately in the trolley and carrying and handling laptops appropriately. These must be checked regularly to ensure no items go missing.

For pupils access to the Internet must always be under adult supervision.

Children and Parents who wish to access the Internet using Department equipment or networks at home (eg taking laptops, i-pads, i-pods home) will be asked to sign and return a copy of the pupil Acceptable Use Policy.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with Department child protection procedures.

e-safety curriculum

The school has an e-safety curriculum which is the most important strand of the overall ICT curriculum. It is taught from reception through to year 6.

- E-safety rules and the AUP will be discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- It is an expectation that all staff adhere to the Department of Education, Sport and Culture's Acceptable Use policy.

Enlisting parents' support

Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Wiki. Links will be made to information for parents to use to support e-safety issues out of school.

Monitoring and Evaluation

Monitoring is the responsibility of the head teacher, the Deputy Head teacher and the ICT co-ordinator.

The effectiveness of the e-safety policy will be evaluated by assessing children's understanding and implementing change if required.