DALRIADA SCHOOL

POLICY DOCUMENT

E-Communication and Acceptable Use of Digital Resources Policy

SECTION A - Pupils

1. **Introduction**

The successful delivery of the Northern Ireland Curriculum places an increasing emphasis on Internet access and ICT use. This document clarifies what is expected of all pupils, with regard to acceptable use of the Internet and other aspects of ICT.

2. **Supervision and Location**

To restrict the possibility of access to unsuitable material the school will use an Internet service provider system that incorporates recognised filtering and control measures. However, there is no present or likely future technical solution that can absolutely guarantee that pupils will never gain access to unsuitable material. The filtering systems used by the school give a very high degree of protection against content of a sexual nature, but other unacceptable material, whether racist, extremist or violent for instance, is difficult to exclude completely.

To increase protection:

a) the effectiveness of the filtering and control measures will be monitored regularly;
b) pupils will normally only have on-line access to the Internet under the direct supervision of a member of staff;
c) Internet access for pupils will be available only on computers in highly used areas of the school where they will be positioned to allow staff to maintain a clear line of vision to their screens;
d) all pupils will be made aware that the school has in place and will use measures to track and record all sites visited, the nature of the searches made, and the content of emails sent and received by them.

3. **Terms and Conditions**

While using the Internet pupils will be asked to adhere to strict guidelines. These guidelines are provided so that pupils will be aware of their responsibilities to themselves and to others. In general, this will require efficient, ethical and legal use of Internet resources. Before pupils gain access to the school's Internet they and their parents/guardian will be asked to sign an undertaking accepting the guidelines.

If a pupil violates any of these provisions, future access could be denied, and serious disciplinary action may be taken by the school. Violations of UK law will be referred to the appropriate authorities.

This policy is linked to the School Behaviour Management, Anti-Bullying and Mobile Phone policies.

4. **Acceptable use of the Internet to support teaching and learning includes:**

   a) The use of email and video-conferencing for communication between pupils in Dalriada and pupils of other schools, between pupils and approved organisations;
   b) The use of the Internet to investigate and research school subjects, cross-curricular themes and topics related to social and personal development;
   c) The use of the Internet to investigate Careers and Further and Higher Education courses;
   d) The use of the Internet to develop pupils' Information and Communications Technology skills (ICT).

5. **Unacceptable use of the Internet includes:**

   a) Playing on-line computer games or using other interactive 'chat' sites unless specifically assigned by the teacher in charge;
   b) Using ICT to upset or harass someone else;
   c) Publishing, sharing or distributing another person's personal information;
   d) Searching for and viewing or saving materials that are not related to the aims of the school or future careers;
   e) Transmission of any material in violation of any legal regulations. This includes, but is not limited to: threatening or obscene material or material protected by a trade secret;
   f) Copying, saving, and/or redistributing copyright-protected material without approval;
   g) Subscribing to any services or ordering any goods or services, unless specifically approved by the school;
   h) Using the school's network in such a way as to disrupt the work of other users (for example, downloading large files during times of peak use, or sending mass email messages);
   i) Obtaining illegal access or entry into other computers;
   j) Vandalism: defined as any malicious attempt to harm or destroy data of any user of the school's network or any external network; this includes, but is not limited to, the uploading/downloading or creation of computer viruses;
   k) Any activity that violates the school's Behaviour Management, Anti-Bullying or Mobile Phone policies.
   l) Activities pertaining to the production of resources in support of Phishing, Pharming, Malware, Blagging, Spyware and Viruses.

   Please note
   The points listed above apply to Internet use via the C2K and legacy systems in school and also to any pupil's personal digital device that can access the Internet.

E-Safety Advice for pupils

The use of ICT, particularly mobile phones and the Internet to deliberately upset someone is on the increase. Cyberbullying is the misuse of social networking sites, Apps and mobile phones to send offensive messages to others via any digital communication device.

a) Keep your C2k password safe. Do not tell other pupils your C2k Password;
b) Do not allow anyone else to log onto the C2k system using your Username and Password;
c) If you receive any offensive emails, or offensive images tell your class teacher or Form Tutor immediately. Do not respond digitally to the communication.
d) When using the Internet in school do not reveal any details, such as personal address, home telephone or mobile telephone number to anyone else in any on-line communication;
e) If you use a social networking site or app, you need to be extremely careful about the information you disclose to others. You could unknowingly reveal personal details that can be seen by many other users.

Here are some useful Websites if you wish to learn more about keeping safe online

https://www.childnet.com/young-people
http://www.digizen.org/kids/
https://www.saferinternet.org.uk/
http://www.bullying.co.uk/cyberbullying

Other Links

Pupils will receive lessons regarding Internet Safety in their ICT and/or Learning for Life and Work classes. Outside agencies may also be used to deliver guidance and advice for pupils and parents.

Advice for Parents

While in school, teachers will guide pupils towards useful Internet sites that provide valuable aids to learning.

The Internet is a valuable source of information and parents are encouraged to ensure that their children continue its constructive use, as it can make a very beneficial contribution to home and school work.

If you have any concerns about your child using the Internet or other forms of e-communication in connection with school, you may find it helpful to consider:

a) Making sure that your child accesses the Internet through a filtered service which will provide protection against inappropriate material, (if you are unsure how this can be done, then please contact the school for help);
b) Setting down general guidelines for access, in a similar way to that for television, films, telephone use, radio and other media;
c) Encouraging your child not to respond to unwelcome, unpleasant or abusive messages and to tell you if they receive such messages;
d) Discussing and agreeing with your child, rules for using the Internet;
e) Being familiar with the Internet sites your child is visiting;
f) Encourage your child to be very cautious before revealing any personal information, such as a photograph, an address, a telephone number, or financial information such as a credit card or bank details in any electronic communication on the Internet.

Young people (and adults) enjoy communicating with their family and friends by using Social Networking Sites. Please ensure that your child is aware that personal information may be seen by users unknown to them;
Photographs posted on social networking sites can often be viewed by users, many of whom may be complete strangers;

Useful Internet Sites for Parents that deal with the potential dangers of the Internet

http://www.digizen.org
http://www.childnet-int.org/KIA/parents
https://www.saferinternet.org.uk/
http://www.bullying.co.uk/cyberbullying
https://ceop.police.uk/safety-centre/

SECTION B - Staff

1. **Introduction**

The successful delivery of the Northern Ireland Curriculum places an increasing emphasis on Internet access and ICT use. This document clarifies what is expected of all school staff, with regard to acceptable use of the Internet and other aspects of ICT.

If a member of staff violates any of these provisions, future access could be denied, and serious disciplinary action may be taken by the school. Violations of UK law will be referred to the appropriate authorities.

This policy is linked to the Discipline (Staff), School Behaviour Management, Anti-Bullying and Mobile Phone policies.

2. **Acceptable Use**

The use of ICT school facilities by staff should be consistent with the aims of the school. On-line activities that contribute to these aims include:

a) the development of staff ICT skills;
b) use of the Internet in teaching and learning;
c) use of the Internet in school administration;
d) communication between members of staff;
e) communication with public authorities such as DENI, ETI and Education Authority
f) communication with Parents;

Using the school networks to send and receive personal email is acceptable, provided this does not include any of the areas set out below under unacceptable use.

3. **Unacceptable Use**

On-line and associated ICT activities in school that are unacceptable include:

a) any posting on the internet without prior authorisation from the Headmaster or a Deputy Head
b) the transmission or reception of any material in violation of any legal regulations. This includes, but is not limited to: threatening or obscene material, or material protected by a trade secret;
c) copying, saving, and/or redistributing copyright protected material, without approval;
d) subscribing to any services or ordering any goods or services for school use, unless specifically approved by the Senior Management of the school;
e) using the school's network in such a way as to disrupt the work of other users (for example, sending mass e-mails);
f) using the school's digital resources (including electricity) for mining of cryptocurrency.
g) gaining unauthorised or illegal access or entry into other computers;
h) any malicious attempt to harm or destroy data of any user of the school's network or any external network; this includes, but is not limited to, the deliberate uploading/downloading or creation of computer viruses;
i) any activity that violates staff disciplinary policies.

4. **Protection for Staff**

Contact with pupils by mobile phone (including group texting) must be for school-related activities only and is only permitted after consultation with the Headmaster or Deputy Heads.

To help protect themselves and to ensure the efficient use of the school's Internet access system, staff will be expected to adhere to the following guidelines:

a) do not allow anyone, other than authorised staff or pupils, to have access to school ICT equipment or connectivity, including access to the school laptops;
b) keep secret any access code or password assigned to them by the school;
c) do not permit pupils to log onto the C2k network using staff usernames and passwords;
d) seek permission from ICT manager before adding or removing software on any of the school's computers;
e) report to a member of senior management any failure of security in the school system/equipment which allows access to inappropriate material;
f) report to a member of senior management any inappropriate material received on-line using the school system/equipment;
g) be aware that the school has in place and will use digital monitoring tools to track and record all sites visited, the nature of the searches made, and content of the emails sent and received;
h) when communicating with pupils in relation to school business staff should use only their staff C2k e-mail address and the pupils' C2K e-mail address.
i) follow GDPR procedures regarding the confidentiality of pupil information.

5. Advice to teachers regarding Social Networking sites

The school strongly recommends that no member of staff should use social networking sites to communicate with pupils. If a teacher wishes to use social networking sites, prior permission must be sought from the Headmaster or Deputy Heads. When using social networking sites, staff are expected to uphold the values and ethos of Dalriada School and at all times safeguard the reputation of the school.

Sources

https://ceop.police.uk/safety-centre/
https://www.saferinternet.org.uk/
https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

Links to other school policies.

This policy is linked to the school policies on:

Child Protection
Health & Safety
Behaviour Management (Pupils)
Use of Reasonable Force
Mobile Phones
Discipline Policy (Staff)
Equal Opportunity Policy

Data Protection Policy

…….…… ……..……..

Date Chair

Adopted by the Board of Governors on 28 November 2019
This document will be reviewed annually by the Board of Governors
This Policy was reviewed by SLT on 18th May 2022