



RBAI e-Safety Policy

Rationale

This policy is to be used in conjunction with the RBAI Pupil ICT and BYOD Acceptable Use Policies and RBAI Staff ICT Acceptable Use Policy.

Devices covered by the policy include any digital or internet-enabled device:

Aims

To highlight the responsibility of the school, staff, governors and parents to educate on and mitigate online and digital risk through reasonable planning and actions.

To educate pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way.

Objectives

e-Safety in the school context:

- is concerned with safeguarding children and young people in the digital world.
- emphasises learning to understand and use new technologies in a positive way.
- is less about restriction and focuses on education about the risks as well as the benefits so that users feel confident online.
- educate on the effects of their online actions on others.
- is concerned with supporting pupils to develop safer online behaviours both in and out of school.
- is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately.

Roles and Responsibilities

Principal

- The Principal has a duty of care for ensuring the safety (including e-safety) of members of the school community.
- The Principal and the Designated Teacher for Child Protection should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff or a pupil.

ICT Co-ordinator

- has a leading role in establishing, reviewing and disseminating the school e-safety policies/documents
- provides training and advice for staff
- liaises with C2k
- liaises with school technical staff

Teachers and support staff are responsible for using digital devices in accordance with the Staff Acceptable Use Policy and are responsible for ensuring that:

- they have an up-to-date awareness of e-safety matters, including cyber security and the current school e-safety policy and practices.
- they have read, understood, and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse to the ICT coordinator and the relevant pastoral staff as per the Behaviour Policy.
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems.
- e-safety issues are embedded in all aspects of the curriculum and other activities.
- pupils understand and follow the e-safety and acceptable use policies.
- pupils have a good understanding of the best cyber practice and behaviours needed in a digital world.
- they monitor the use of digital technologies in lessons and other school activities (where allowed) and implement current policies with regard to these devices.

Designated teacher for child protection should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with others
- potential or actual incidents of grooming
- cyber-bullying
- cybercrime
- inappropriate use of social media including online gaming

Pupils are responsible for using digital devices in accordance with the Pupil Acceptable Use Policy.

Parents/Guardians play a crucial role in ensuring that their children understand the need to use digital devices in an appropriate way. RBAI will take every opportunity to help parents understand these issues through parents' evenings, written and online communications, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events.
- appropriate use of social media in relation to the school.
- their children's personal devices in the school.

Education of Pupils

Staff are underpinning the following knowledge and behaviours:

- How to evaluate what they see online to enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid, or acceptable.
- How to recognise techniques used for persuasion, including misinformation and disinformation, criminality, grooming and manipulation.
- How to protect themselves from cybercrime.
- The ways in which games and social media companies try to keep users online longer (persuasive or sticky design).
- Grooming and manipulation techniques used by criminals.
- The ways to protect themselves from a range of cybercrimes.
- What acceptable and unacceptable online behaviour look like.
- Upholding the school value of respect when using digital technology.
- How to identify online risks including how and when to seek support, in line with wider school policies.
- How to report inappropriate contact or content for various platforms and apps.

Risk assessment

RBAI staff need to mitigate against risks arising from the use of digital technology. A risk assessment should be conducted before any new technology or digital platform is introduced.

Online activity & personal safety

This section covers elements of online activity that could adversely affect a pupil's personal safety and are addressed through the preventative curriculum.

- **Abuse (online)** including cyberbullying.

Some online behaviours are abusive. They are negative in nature, potentially harmful and in some cases can be illegal. It is important that pupils are encouraged to report incidents of cyber-bullying and/or crime to both the school and, if appropriate, the PSNI to ensure the matter is properly addressed and the behaviour ceases.

Staff should also keep good records of cyber-bullying incidents, following the RBAI Anti-Bullying Policy (and the Additional Guidance for Staff) to monitor the effectiveness of their preventative activities, and to review and ensure consistency in their investigations, support and sanctions.

- **Harassment, bullying, trolling and intimidation.**
- **Online radicalisation.**
- **Online Challenges** (these acquire mass followings and encourage others to take part in what they suggest. while some will be fun and harmless, others may be dangerous and or even illegal).
- **Content which incites violence**

- **Fake profiles**
- **Grooming**
- **Live streaming** (showing a video of yourself in real-time online either privately or to a public audience) carries risk when carrying it out and watching it, e.g., for example, there is no way of knowing what will come next and so this poses a risk that a user could see something that has not been deemed age appropriate in advance.
- **Pornography**
- **Unsafe communication** (Knowing different strategies for staying safe when communicating with others, especially people they do not know or have never met.)

Wellbeing

This section covers the elements of online activity that can adversely affect a pupil's wellbeing.

- **Impact on confidence**
- **Impact on quality of life, physical and mental health, and relationships**
- **Reputational damage** (individual and school)

Vulnerable pupils

Any pupil can be vulnerable online, and their vulnerability can fluctuate depending on their age, developmental stage and personal circumstance. However, there are some pupils, for example, looked after children and those with special educational needs, who may be more susceptible to online harm or have less support from family or friends in staying safe online. The SENCO will assist with tailoring the provision for such pupils.

These guidelines are intended to help a school make explicit the expectations of the school on pupil use of digital technology and the risks that can occur in school and on school grounds. mobile phones and the restrictions which are placed on their use in school and on school grounds. The guidelines sit alongside the Acceptable Use Policy which all pupils sign, and is shared with parents and carers. They also give clear guidance to staff, pupils and parents about the consequences for breaches of the guidelines.

Access to the Internet via the C2k Education Network is fully auditable and reports are available to the school principal.

Reviewed May 2024

Next review May 2026

Appendix 1 Definitions (DENI circular 2013/25)

- **e-Safety** is short for electronic safety.
- **Internet Filtering** - Improved Websense filtering will give schools the flexibility to control and develop their own Internet Filtering Policy. Individual schools may now select to fully delegate management of their filtering policy to a nominated member of staff by signing up to C2k delegated filtering access. This nominated user will receive additional training for this responsibility and can further amend the local filtering policy to the needs and demands of the school. This is in direct response to feedback from schools, who wish to access more internet sites to enhance teaching and learning. However, there are a number of agreed locked down sites that can never be overridden by the local school policy.
- **Meru Wireless** - Meru Wi-Fi will provide increased wireless coverage and improved speed. Meru supports multiple devices and school controlled secure guest access and allows schools to plan for and implement a further purchase by the school or/and a 'Bring Your Own Device' policy.
- **Cloud Storage** - Data and information will be stored on the Cloud in the new service and no longer in the school itself. This means it can be securely accessed from any location removing the need to carry data and files on insecure data pens and portable devices.
- **Personal Devices** - Schools will be able to explore the introduction of new internet enabled devices to support teaching and learning.

Appendix 2 Legal Framework

Notes on the legal framework

This section is designed to inform users of potential legal issues relevant to the use of electronic communications.

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. Please note that the law around this area is constantly updating due to the rapidly changing nature of the internet.

Public Order (N.I.) Order 1987

This Act makes it a criminal offence to stir up hatred or arouse fear. Fear and Hatred both mean fear/hatred of a group of persons defined by reference to religious belief, colour, race, sexual orientation, disability, nationality or ethnic or national origins

Criminal Justice (No2) (N.I.) Order 2004

Commonly referred to as N.I. 'Hate Crime' legislation. This empowers courts to impose tougher sentences when an offence is aggravated by hostility based on the victims actual or presumed religion, race, sexual orientation or disability.

Protection of Children (N.I.) Order 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in Northern Ireland. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences (N.I.) order 2008

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet). It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff etc fall in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission

Protection from Harassment (N.I.) Order 1997

Article 3. This legislation can be considered where a person is pursuing a course of conduct which amounts to harassment. This includes alarming a person or causing a person distress. This course of conduct must be on more than one occasion

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 - 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use

of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Criminal Justice and Immigration Act 2008

Sec 62-68 Includes the Coroners and Justice Act. It is an offence to possess a drawing or painting which depicts a child in an indecent pose or participating in an indecent act.

Section 63 offence to possess “extreme pornographic image”

63 (6) must be “grossly offensive, disgusting or otherwise obscene”

63 (7) this includes images of “threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead” must also be “explicit and realistic”. Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyberbullying/Bullying:

- Head teachers have the power “to such an extent as is reasonable” to regulate the conduct of pupils off site.
- School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti bullying policy.

Addressing Bullying in Schools Act (NI) 2016

Statutory guidance from the Department of Education (NI): Methods of Bullying 1.— (1) In this Act “bullying” includes (but is not limited to) the repeated use of— (a) any verbal, written or electronic communication,

It defines **Cyber bullying** as *an aggressive, intentional act carried out by an individual or group against a target using, for example, electronic forms of contact and online platforms.*

Whilst cyber-bullying may appear to provide anonymity for the person exhibiting bullying behaviour, most messages can be traced back to their creator and pupils should be reminded that cyber-bullying can constitute a criminal offence. The following may also cover different elements of cyber-bullying behaviour:

- Protection from Harassment (NI) Order 1997
<http://www.legislation.gov.uk/nisi/1997/1180>
- Malicious Communications (NI) Order 1988
<http://www.legislation.gov.uk/nisi/1988/1849>
- The Communications Act 2003
<http://www.legislation.gov.uk/ukpga/2003/21>

General Data Protection Regulation 2018

- This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
- This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
- The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Online safety Act 2023

This contains a range of measures intended to improve online safety in the UK, including duties on platforms about having systems and processes in place to manage harmful content on their sites, including illegal content.

Appendix 3 Relevant DENI documents

This policy is cognisant of the following DENI publications:

DE Circular 2007/01: Acceptable Use of the Internet and Digital Technologies in Schools

DE Circular 2011/22: Internet Safety (Addendum to 2007/01)

DE Circular 2013/25: eSafety Guidance

DE Circular 2016/26: Effective Educational Uses of Mobile Digital Devices

DE Circular 2016/27: On line Safety

DE Circular 2017/04: Safeguarding and Child protection in Schools – A Guide for Schools

Appendix 4 Related RBAI Policies

Positive Behaviour & Discipline Policy

Anti-Bullying Policy

Computer Acceptable Use Policy for Pupils

Bring Your Own Device Policy

Staff ICT Acceptable Use Policy

Safeguarding & Child Protection Policy

AI Policy

Data Protection Policy