The Royal Belfast Academical Institution

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:
Mobile phones
Tablets (including IOS, Android & Windows-based devices)
Lap tops & Multi-function devices
Notebooks
e-readers
Smart watches that are web-enabled

Aim

To highlight the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. e-Safety covers not only internet technologies, but also electronic communications via mobile phones, games consoles and wireless technology.

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;
- is concerned with supporting pupils to develop safer online behaviours both in and out of school; and
- 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, though the day to day responsibility for e-safety will be delegated to the ICT co-ordinator.
- 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.

ICT Co-ordinator

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with C2k
- liaises with school technical staff

Teachers and support staff are responsible for using the RBAI technology systems 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 and of 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 or problem to the ICT coordinator and Pastoral Vice Principal
- 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 research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc 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 adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils are responsible for using the RBAI technology systems in accordance with the Pupil Acceptable Use Policy.

Parents/Guardians play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. RBAI will take every opportunity to help parents understand these issues through parents' evenings, 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
- access to parents' sections of the website / VLE
- their children's personal devices in the school.

Education of Pupils

The education of pupils in e-safety is therefore an essential part of the RBAI e-safety provision. Pupils need the help and support of the school to recognise and avoid e-safety risks and build their resilience.
E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum will be provided in the following ways:

- A planned e-safety curriculum will be provided as part of ICT classes and will be regularly revisited

- Key e-safety messages will be reinforced as part of a planned programme of assemblies (e.g. Safer Internet Day) and Registration group activities (Registration and PD period)
- Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils will be helped to understand the need for the Pupil Acceptable Use Policy and encouraged to adopt safe and responsible use both within and outside school
- Staff will act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit

Rules for the acceptable use of a mobile device in school by pupils

Pupils are permitted to bring mobile devices into school. If they choose to do so it is on the understanding that they agree with the following limitations on their use, namely:

1. Mobile devices must be switched off at all times during the school day, including break and lunchtimes, and remain off whilst students are on the school premises. The device must be kept out of sight during lessons. There are two exceptions to rule 1: sixth form access in the Sixth Form Centre Common Room; Language students in Years 11-14 during class when instructed and supervised by their language class teacher.
2. No student may take a mobile device into a room or other area where examinations are being held. This includes smart watches that are web-enabled.
3. The security of a device will remain the pupil's responsibility in all lessons including PE/Games lessons.
4. Content on the device (e.g. messages, emails, pictures, videos, sound files) will be shown to the vice principal/principal by reasonable request. If a student refuses then the parents will be contacted and the mobile device confiscated.

Risk assessments (See Appendix 3)

Schools need to perform risk assessments on the technologies within their school to ensure that they are fully aware of and can mitigate against the potential risks involved with their use. Pupils need to know how to cope if they come across inappropriate material or situations online.

Cyberbullying

Cyber Bullying can take many different forms and guises including:

- Email – nasty or abusive emails which may include viruses or inappropriate content.
- Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.
- Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user's profile.
- Online Gaming – abuse or harassment of someone using online multi-player gaming sites.

- Mobile Devices – examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people.
- Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.

It is important that pupils are encouraged to report incidents of cyber-bullying 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.

These guidelines are intended to help a school make explicit the expectations of the school on pupil use of 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.

Dealing with breaches of the Guidelines

Misuse of a mobile device will be dealt with using the same principles set out in the Positive behaviour & Discipline Policy, with the response being proportionate to the severity of the misuse.

The Vice Principal/Principal will deal with serious incidents of misuse, particularly where there has been a victim of cyberbullying.

Pupils should be aware that serious misuse may lead to the confiscation of their mobile device, communication with parents and the imposition of other sanctions up to and including exclusion from school. If the offence is criminal in nature it will be reported to the PSNI.

Where it is deemed necessary to examine the contents of a mobile device this will be carried out by the Vice Principal/Principal. The action will be properly recorded in case it later becomes evidence of criminal activity. The record will include the time, who was present and what is found.

Unacceptable use

The school will consider any of the following to be unacceptable use of a mobile device and a serious breach of the school's Positive behaviour & Discipline Policy resulting in sanctions being applied:

- Photographing or filming staff or other pupils without their knowledge or permission;
- Photographing or filming in toilets, swimming pool and changing rooms and similar areas;
- Bullying, harassing or intimidating staff or pupils by the use of text, email or multimedia messaging, sending inappropriate messages or posts to social networking or blogging sites
- Refusing to switch a mobile device off or handing over the mobile device at the request of a member of staff.

Using a mobile device outside school hours to intimidate or upset staff and pupils will be considered a breach of these guidelines in the same way as unacceptable use which takes place in school time.

Sanctions

Pupils and parents are notified that appropriate action in accordance with the Positive Behaviour & Discipline Policy will be taken against those who are in breach of the acceptable use guidelines. In addition

pupils and their parents should be very clear that the school is within it rights to confiscate the mobile device where the guidelines have been breached.

Where the mobile device has been used for an unacceptable purpose

The Principal or a designated staff member will have the right to view files stored in confiscated equipment and will seek the cooperation of parents in deleting any files which are in clear breach of these Guidelines unless these are being preserved as evidence.

If required evidence of the offence will be preserved, preferably by confiscation of the device and keeping it secure or by taking photographs of the screen.

Advice can be sought from the Education Authority Child Protection Team and/or the PSNI. School should consider whether an incident should be reported to the school Designated Teacher.

The designated staff member should monitor repeat offences to see if there is any pattern in the perpetrator or the victim which needs further investigation in line with the school's Anti-Bullying Policy.

Communication of the e-Safety Policy

- All users will be informed that C2k network internet access and email use will be monitored.

Email security

In the school context (as in the business world), email should not be considered private. C2k recommend that all staff and pupils should be encouraged to use their C2k email system. It is strongly advised that staff should not use home email accounts for school business.

The C2k Education Network filtering solution provides security and protection to C2k email accounts. The filtering solution offers scanning of all school email ensuring that both incoming and outgoing messages are checked for viruses, malware, spam and inappropriate content.

Internet security

Staff and pupils accessing the Internet via the C2k Education Network will be required to authenticate using their C2k username and password. The C2K authentication process will provide Internet filtering via the C2k Education Network solution.

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

Reviewed Dec 2019

Appendix 1 Definitions (DENI circular 2013/25)

1. **e-Safety** is short for electronic safety.
2. **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.
3. **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.
4. **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.
5. **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 ethic 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.

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner’s Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

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.

Cyber-bullying

Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils should be reminded that cyber-bullying can constitute a criminal offence. While there is no specific legislation for cyber-bullying, the following may 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

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

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

Appendix 5

Proposed responses to e-safety incidents by children matrix

The following matrix offers examples of typical incidents and suggestions as to possible responses.

No.	Activity	Hazard	Likelihood	Impact	Score	Further controls
1.	Internet browsing	Access to inappropriate/illegal content - staff	1	3	3	
1.	Internet browsing	Access to inappropriate/illegal content - pupils	2	3	6	
2.	Blogging	Inappropriate comments	2	1	2	
2.	Blogging	Using copyright material	2	2	4	
3.	Pupil laptops	Pupils taking laptops home – access to inappropriate/illegal content at home	3	3	9	Risk management needed by ICT department
4.	BYOD	Inappropriate/illegal content brought into school	3	3	9	Risk management needed by ICT department

Risk Assessment

Likelihood: How likely is it that the risk could happen (foreseeability).

Impact: What would be the impact to the school (e.g. this could be in terms of legality, reputation, complaints from parents, reporting in press etc.)

Likelihood and Impact are between 1 and 3, 1 being the lowest.

Multiply Likelihood and Impact to achieve score.

LEGEND/SCORE: **1 – 3 = Low Risk**
4 – 6 = Medium Risk
7 – 9 = High Risk

Owner: The person who will action the risk assessment and recommend the mitigation to the Principal and Board of Governors. Final decision rests with Principal and Board of Governors.