Royal School, Armagh

Acceptable Use of ICT Policy

Related Documents:
DE Circular 2016/27
DE Circular 2016/26
DE Circular 2015/17
DE Circular 2013/25
DE Circular 2011/22

Acceptable Use of ICT Policy

A whole school networked infrastructure, incorporating a C2k LAN and Virtual Learning Environment (VLE), along with other electronic class-based resources such as tablets, is available to staff and pupils at the Royal School Armagh (RSA).

The staff at RSA strongly believes in the educational value of such electronic services and recognises their potential to support teaching and learning within the NI curriculum and at the same time support the integration of ICT within and across all subjects. Every effort will be made to provide quality experiences to pupils and teachers using this networked infrastructure, however, inappropriate and/or illegal interaction with any information service is strictly prohibited. *This also applies to personal electronic devices when used within the jurisdiction of the school (and also applies to use whilst on school trips).*

Please read this document carefully. Listed below are the provisions of this agreement. If any student violates these provisions, access to the C2k network (including the Internet), VLE and other devices will be denied and the pupil will be subject to disciplinary action.

Terms and Conditions of This Agreement

1. Personal Responsibility

As a representative of the school, each pupil must accept personal responsibility for reporting any misuse of the network to a staff member. Misuse may come in many forms, but it is commonly viewed as any message(s) sent or received that indicate or suggest pornography, unethical or illegal requests, racism, sexism, inappropriate language, any use which may be likely to cause offence (such as cyber bullying), emotional upset and other issues described below.

2. Acceptable Use

The use of electronic services must be in support of education and research in accordance with the educational goals and objectives of RSA. Each pupil must be personally responsible for this provision at all times when using the electronic information services.

- Use of other networks or computing resources must comply with the rules appropriate to that network.

- Transmission of any material in violation of any United Kingdom or other national laws is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material or material protected by trade laws.

- Use of commercial activities by for-profit organisations is generally not acceptable.

3. Privileges

The use of the Internet and other electronic services is a privilege and inappropriate use will result in that privilege being withdrawn. Pupils with access to the Internet will participate in a discussion with a member of the school staff as to proper behaviour and use of the facilities. RSA staff will rule upon inappropriate use and may deny, revoke or suspend usage.

4. Network Etiquette and Privacy

Each pupil is expected to abide by the generally accepted rules of network etiquette. These rules include, but are not limited to the following:

1. USE APPROPRIATE LANGUAGE. Remember that you are a representative of the school on a global public system (supporting Web 2.0, email or internal messaging, for example). You may be the only one logged onto your computer, but what you say and do can be viewed by others. Never swear, use vulgarities or any other inappropriate language. Illegal activities of any kind are strictly forbidden. Be internet-wise and remember that your activity will leave a digital foot-print.

2. BE POLITE. Never send or encourage others to send abusive messages. NEVER engage in cyber-bullying.

3. PRIVACY. Do not reveal any personal information to anyone, especially the home address or personal telephone number of yourself or any other pupils. DO NOT upload pictures of you or your friends unless agreed by the school through extra-curricular or class-based activities.

4. NEVER MEET with someone you have met on the Internet: they may not be who they say they are. If you are worried speak to your parent, carer or a teacher. If you are being blackmailed or threatened you must speak to your parent, carer or a teacher.

5. PASSWORDS. Do not reveal your password to anyone. Furthermore, with regard to password use on the network infrastructure (C2k and VLE) the following security principles should be applied by all users.

- *Passwords should not be obvious. For example, words such the user’s name or the name of a favourite pop group should not be used.*
- *Passwords should be at least eight characters long.*
- *Passwords should contain upper and lower case letters as well as numbers and special (ASCII) characters.*
- *Passwords should remain confidential.*
- *Passwords should never be written down.*
- *Passwords should be regularly changed.*

If a user believes their password is known by someone else then they should see the ICT technician or an ICT teacher immediately or alternatively inform a member of staff.

6. OTHER CONSIDERATIONS:

(a) Keep your message brief and to the point.
(b) Proof read your message to ensure that it is error free and easy to understand.
(c) Remember that humour and satire are very often misinterpreted.
(d) Respect the rights and beliefs of others.
(e) Be aware of fraudulent activity on all electronic accounts and be "internet wise". Never give your username or password in response to email (phishing) requests.

5. Services

RSA makes no warranties of any kind whether expressed or implied, for the network service it is providing. RSA will not be responsible for any damages suffered whilst on this system. These damages include loss of data as a result of delays, non-deliveries, mis-deliveries or service interruptions caused by the system or elements of the system, or your errors or omissions. RSA specifically denies any responsibility for the accuracy of information obtained via its Internet services.

6. Security

Security on any computer system is a high priority because there are so many users. If you identify a security problem, notify a member of the ICT staff at once. Never demonstrate the problem to another student. All use of the system must be under your own username and password unless specifically directed by a member of staff. Remember to keep your password private. Do not share it with friends. Anyone caught disclosing passwords may have their access denied and may be subject to disciplinary action. Any user identified as a security risk may be denied access to the system and be subject to disciplinary action.

7. Vandalism

Vandalism is defined as any malicious attempt to harm or destroy any equipment or data of another user or of any other networks that are connected to the system. This includes, but is not limited to, the uploading or creation of computer viruses, the wilful damage of computer hardware, whether connected to the network or not and the deletion of data from its place of storage.

8. Online Ordering systems

One of the many facilities available via the Internet is the ability to order goods and services whilst online; however, questions have been raised with regard to the issue of security of online credit card ordering etc. Because of the security and other ethical issues attached to this facility, RSA has a moral responsibility in this area. It is therefore strictly forbidden for pupils to use the Internet for ordering goods or services regardless of their nature. In addition, it is also forbidden for pupils to subscribe to any newsletter, catalogue or other form of correspondence via the Internet, regardless of its nature.

9. Electronic Mail

Electronic mail (email) is accessible within C2k and is also widely available via the Internet. Pupils are expected to use this facility in a responsible manner. The sending or receiving of any email, which contains any inappropriate material, is strictly forbidden. This material includes, but is not limited to, pornography, unethical or illegal requests, racism, sexism, inappropriate language or any use which may be likely to cause offence. Disciplinary action will be taken in all cases. It is also forbidden to send large volume emails (SPAMMING).

The C2k system monitors all outgoing and incoming email. The C2k system also contains an email filtering facility and any email which is considered to have inappropriate content such as viruses, dangerous attachments and SPAM will be blocked and held by the C2k system. All blocked emails will be scrutinised and will only be forwarded to the addressee(s) when their content falls within the email policy of the school and C2k (see above). This applies to all outgoing and incoming email sent and/or received by ALL users on the C2k system.

- At RSA all pupils are encouraged to use their C2k email system responsibly. It is strongly advised that staff should not use home email accounts for school business (*see related Data Protection and Security Protocols Policy*).

- 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.
- Where staff and pupils use non C2k emails accounts, RSA will audit and monitor usage through the service provider(s) firewalls.
- Pupils may only use C2k email accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- The forwarding of chain mail or spam is not permitted.
- Pupils must not transmit photographs or video of themselves, other pupils or staff through email.

10. Cyber-bullying

Whilst it is recognised that each of the social media technologies can offer much to pupils' learning, RSA is aware that each brings its own unique issues and concerns. Each social media technology that is to be utilised is risk assessed in the context of use within a teaching and learning and pastoral context.

Through curriculum based instruction, pupils are made aware of the unacceptable aspects of cyber-bullying via electronic methods of communication (which has the potential to originate both in and out of RSA's jurisdiction). *This form of bullying is considered within RSA's overall anti -bullying policy and pastoral services as well as the eSafety policy.*

At RSA pupils are made aware that cyber-bullying can take many different forms and guises including the ***inappropriate and unacceptable use*** of the following:

- *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 Phones – 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.*

Pupils will be made aware that whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils are 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 and can be used as a source of reference:

- 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

At RSA pupils are encouraged to report incidents of cyber-bullying to both the school and, if appropriate, to the PSNI to ensure the matter is properly addressed and the behaviour ceases.

RSA will keep detailed records of cyber-bullying incidents and will monitor the effectiveness of their preventative activities, and will review and ensure consistency in all investigations, support and sanctions.

11. Social Networking

It is recognised, as referenced in the previous cyber-bullying section, that recent changes to the criteria used to allow information to be uploaded to social media sites (outside the school environment) raises particular concerns for children and young people, particularly in relation to access to social media sites outside the C2k service.

At RSA care will be taken when making use of social media for teaching and learning. It is recognised that each of the social media technologies can offer much to pupils' education but each brings its own unique issues and concerns. Each social media technology that is to be utilised will be risk assessed in the context of each area of use. Therefore pertinent areas of focus within the social networking remit are identified.

- The school C2k system will block access to social networking sites unless utilised by the teacher only.
- RSA recognises that some pupils will use social networking sites outside school; and they will be advised never to give out personal details of any kind, which may identify them or their location. Pupils are advised not to meet with those they have met on social networking sites.
- If pupils are legal members of such social networking sites (based on conditions of joining), all pupils will be advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are asked to report any incidents of cyber-bullying (or bullying) to the school.

12. Related RSA ICT documents (available as separate publications):

- *Acceptable Use Policy ICT – Pupils RSA*
- *Acceptable Use Policy ICT – Staff RSA*
- *Acceptable Use Policy and Bring Your Own Device Policy RSA*
- *Data Protection and Security Protocols Policy RSA*
- *e-Safety Policy RSA*
- *ICT Use Across the Curriculum RSA*
- *Safe Use of the Internet at Home Policy RSA*

11. Related DENI Circulars reviewed in the development and revising of this policy (available as separate publications):

DE Circular 2016/27
DE Circular 2016/26
DE Circular 2015/17
DE Circular 2013/25
DE Circular 2011/22

Revised April 2017

Note: Use of ICT as defined in this policy is subject to the existing and future school policies on Child Protection, Anti-Bullying and Discipline. This policy is reviewed annually.