Ardscoil Rath Iomgháin
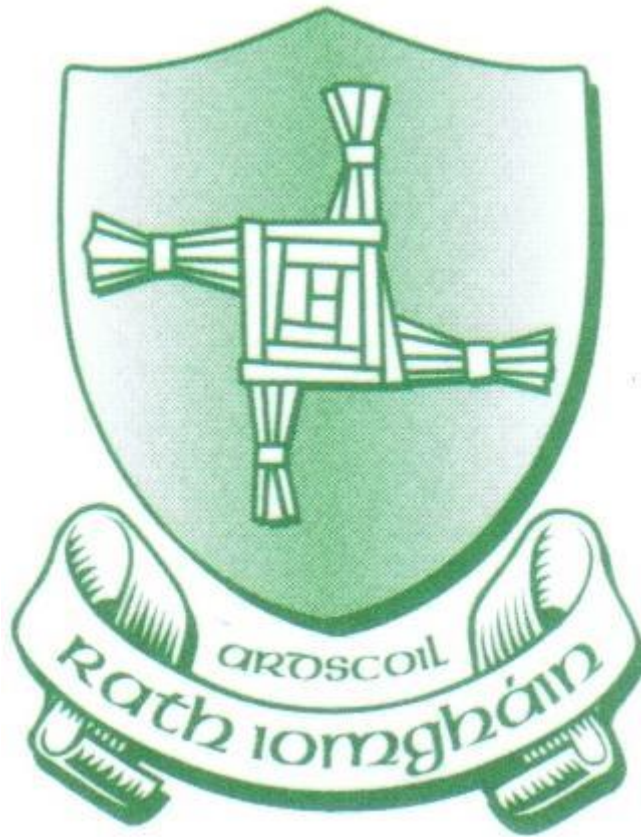

Information and Communications

Technology

Acceptable Usage Policy

(June 2014)

Table of Contents

1. The Purpose of this Policy

ArdsScoil Rath Iomgháin owns and operates a variety of computing systems and services, these facilities are provided in the support of the programs provided by Ardscoil Rath Iomgháin and are to be used for education, research, academic development and public services only. All users of these systems are responsible for seeing that these computing facilities are used in an effective, efficient, ethical and lawful manner.

This Document establishes the rules and regulations that define acceptable use of these systems. Unacceptable use is prohibited, and is grounds for loss of computing privileges, as well as discipline or legal action.

2. Scope

This policy applies to all staff, students, volunteers and other users of Ardscoil Rath Iomgháin regardless of status, whether directly or indirectly employed by Ardscoil Rath Iomgháin, or otherwise under its control (hereafter known as "User").

The policy also applies to all information systems used by Ardscoil Rath Iomgháin wherever located and for whatever purpose used, and whether operated by Ardscoil Rath Iomgháin or by an outside body on its behalf.

This includes:

- All systems and information created, held or used on Ardscoil Rath Iomgháin's main computer systems, school network, local area networks and standalone personal computers, including home, laptop PCs, PDA devices and tablets.

- Electronic mail, voice mail, telephone, video-conferencing and other facilities used both for voice and data transmission, internal and external.

- Internet technologies.

3. Policy Statements

3.1. Accounts

Accounts will be issued and revoked solely by the ICT Service Team. Users may not use an account assigned to another user without express permission from the ICT Service Team. Users are responsible for the proper use of the account including but not limited to all work carried out through and transmitted to and from the account issued and for the maintenance of files and folders created with said account.

All users are required to have set a password of minimum 5 characters on the account and may not disclose this password to any person.

It is advised that users use a combination of UPPER and lower case letters and numbers to make up this password.

The use of the word "password" as a password is **strictly forbidden**.

3.2. Confidentiality

Programs and files are confidential unless they have been made available, with written permission, to other authorised users. The ICT Service Team reserves the right to access all information stored on all ICT Facilities provided by Ardscoil Rath Iomgháin. Every effort is made to insure the privacy of a user's files. However, if policy violations are discovered, they will be reported to the Principal or Deputy Principal(s) immediately.

The confidentiality of any message or file should not be assumed. Even when a message is erased it is still possible to retrieve and read that message. If any breach of this policy is observed, then disciplinary action up to and including dismissal/expulsion may be taken.

3.3. Monitoring

Users must be aware that all their computer activity is tracked and logged for reference purposes. These individual user logs and associated files may be accessed at any time by the ICT Service Team. If policy violations are discovered they will be reported immediately.

Electronic communication facilities (such as email and Instant messaging) are for school related activities only. Fraudulent, harassing or obscene messages and/or materials are not to be sent or stored.

3.4. System Performance

No one should deliberately attempt to disrupt the performance of the schools ICT system or to deprive authorised users of resources and/or access to any of the schools ICT Systems.

3.5. Unauthorised Access

Any vulnerabilities in the ICT security systems or knowledge of special passwords should not be used to damage ICT systems, obtain extra resources, take resources from other users, gain access to systems or use systems for which proper authorisation has not been given.

Any vulnerabilities or special passwords discovered should immediately be reported to the ICT Service Team.

3.6. Bring Your Own Device (BYOD)

Users using their own devices in school are governed by this policy. In addition users will not connect their personal device to the schools network (wall sockets or WIFI) or other equipment without prior registration of the device with the ICT Service Team at the time of introduction to the school and re-registration at the start of the academic year thereafter.

Unregistered devices may be confiscated. Any access to the network from smart phones, ipads or other digital devices must be used with the username and password of the owner of the device. Any access by another user on a device not owned by them will be considered as an offence and both the owner and user will be considered in breach of this policy.

3.7. Copyright

Ardscoil Rath Iomgháin's ICT facilities will not be used to copy, use or distribute illegally obtained (pirated) copyrighted materials except as permitted by law or by the contract with the owner of the copyrighted material(s).

3.8. Virus Protection

Computer viruses are items of software that attach themselves to other legitimate items of software or data, without the consent of the computer user, and are programmed to spread themselves onto other computers, often to cause disruption or damage. It is essential that all users play a part in protecting the network from the presence of viruses.

It is the policy of the school to run up to date virus protection software on all computers. This software will automatically report the presence of most known viruses. Any user who receives

an on-screen warning from this software (these are very clear and explicit) should stop all use of the computer immediately and report the occurrence to the ICT service team.

Viruses can attach themselves easily to removable storage media and this is one of the main ways in which they spread. The software used to prevent students from tampering with computer settings will also, to some extent, prevent them from accessing these removable media. However this is not totally secure. Furthermore there are instances in which students and staff will want to transfer data to and from the network on removable media, e.g. as a means of submitting homework. To allow for this and still ensure system security it is the school's policy that all removable media must be virus scanned before being accessed through any computer on the network. These must be re-scanned again each time they are used in computers outside the network.

Users are **strictly forbidden** to attempt to download viruses themselves.

3.9. Legal obligations and Legislation

The use of all ICT systems, resources and associated applications are subject to Irish, European and international laws. Any illegal use will be dealt with appropriately through the schools disciplinary process. (Code of Behaviour Policy)

The school reserves the right to report any actual or potential illegal violations of these laws to the relevant authorities.

Ardscoil Rath Iomgaháin is committed to ensuring that it complies with all following legislations in relation to the use of the Internet

- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video Recording Act 1989
- Data Protection Act 1989
- Data Protection (amendment) Act 2003

The school makes every effort to ensure that personal information is maintained in a manner which is accurate, relevant and is held securely at all times. all those maintaining records on behalf of the school are required to ensure that they adhere to the provisions of the Data Protection Acts.

Copies of the above mentioned acts are available from the school on request and we ask that all users and parents familiarise themselves with these acts.

3.10. Use of Recording Devices

The use of electronic recording devices to facilitate specific institutional and administrative services is permitted based on established policies and practises. Such uses include but are not limited to the schools or KWETB's administrations systems and related uses, school or KWETB publications and broadcast facilities, athletics programs and theatrical productions, scheduled distance learning classes, video conferences, digital streaming class content (live or recorded) and the recording of Audio, Video or still images (photos) of classes or related events by Audio And Visual Media Distribution services.

Electronic devices may be used to record classes, presentations, interviews or similar activity with prior permission of the individual being recorded and/ or the schools or KWETB's management this permission does not extend to any other person that may be present. Absence of permission may constitute copyright infringement and will be dealt with in line with the schools code of behaviour and/or local, European and international law. Verbal permission may be sufficient for recording within a class or meeting for personal use. However written permission must be obtained prior to the recording and or distribution of someone's image or speech over the airwaves, in public on the web, as part of a class assignment or any school sponsored activity or program.

It is the responsibility of the user, host, event organiser(s) or department to provide notification and obtain the necessary permissions in advance or at the time of the recording and or transmission.

3.10.1. Expectations of Privacy

Taking photos and or making audio or video recordings without permission in **ANY** contexts in which the person has a reasonable expectation of privacy is prohibited. Such physical areas on the school grounds include but are not limited to private offices, restrooms, changing rooms, labs, classrooms and conference rooms. In such areas, permission must be granted by all persons being photographed or recorded

3.10.2. Surveillance Equipment and software

Surveillance equipment and software may be placed on the school grounds and monitored by authorised personnel to prevent or deter crimes and protect public safety and to facilitate the investigation of criminal activities or violation of the

schools policies. The use of surveillance will be in accordance with the schools code of behaviour, Data protection and CCTV Policy and local, European and international law.

3.11. Internet

3.11.1. General

Users must be aware that all internet activity is actively monitored and logged, as part of this Ard scoil Rath Iomgháin employs internet filtering systems to minimise the risk of exposure to inappropriate materials (including but not limited to pornography, extreme violence, terrorism and copyright piracy).

Users will not intentionally try to bypass these systems to visit sites containing obscene, illegal, hateful or otherwise objectionable materials. All Users are required to report immediately any accidental accessing of inappropriate materials to the ICT Service Team, Principal or Deputy Principal(s).

Users will not reveal their own or another person's personal details, such as addresses, telephone numbers or pictures.

The organising of face-to-face meetings with someone via the internet by students is **strictly forbidden.**

All Users will be provided with training in the area of internet safety and expected online behaviour.

3.11.2. Email

All users are provided with a school email address. These accounts are only to be used for school or educational business.

Teachers are expected to only use school email accounts when communicating professionally with parents, students and other partners in education or other significant bodies regarding school or educational business.

Students will use school email accounts under supervision or with the permission of a teacher to communicate approved work to or from the school. Sending and receiving email attachments is subject to permission from a teacher.

Non-school related business should be conducted using non-school email accounts.

Users will not send any materials that are illegal, obscene, discriminatory, racist, homophobic, defamatory or intended to annoy, intimidate or (cyber)bully another person.

Should you receive any offensive, unpleasant, harassing or intimidating messages via email you are requested to inform the Principal/Deputy Principal(s) or The ICT Service Team immediately.

3.11.3. Internet Chat

On occasion students may be given access to chat rooms, discussion forms or other electronic communication forums that have been approved by, or set up by the school.

These communication forums will only be used for educational purposes and will always be supervised.

As stated before the organising of face-to-face meetings with someone via the internet by students is **strictly forbidden**.

3.11.4. School website

Users will be given the opportunity to submit projects and/or school works for publication on the school website. All works will be published in accordance with the policies regarding content that can be published on the school website.

The school website is regularly checked to ensure that there is no content which could compromise the safety or integrity of our users.

Any area which allows user-generated content such as comments will regularly be checked to ensure that they do not contain personal details or are intended to annoy, intimidate or (cyber)bully another person.

Publication of work will be co-ordinated by teachers and the ICT Support Team.

The school endeavours to use digital photographs, audio and/or video clips focusing on group activities on the school website. Content focusing on individual students will only be published on the school website with parental permission.

Personal student details such as home address and contact details **will never be published** on the school website.

Users will continue to own the copyright on any work published.

Copying private messages to another person without the author's explicit permission is a breach of confidentiality and in breach of this policy.

3.11.5. Other Internet Technologies and Services

New and emerging technologies will be examined for educational benefit and a risk assessment will be carried out before the use in the school is allowed.

A list of approved services can be requested from the ICT Service Team.

Staff wishing to use new technologies not on the approved list, will need to submit a request to the ICT Service Team well in advance for a risk assessment to be carried out before permission can be given. Staff will make every effort to ensure that all material shown is suitable to the relevant age group in classes. They will also aim to ensure that no material shown in classes will cause offence to any students.

The appropriate use of **Mobile phones** is governed by Code of Conduct and the school's mobile phone policy.

4. ICT Use in general

Users must not represent personal opinions or views as those of Ardscoil Rath Iomgháin

Users will not pretend to be someone else

Users will not use school resources to forward chain emails.

IT facilities should not be used to make or post indecent remarks, proposals or any material which may bring the school into disrepute. Users are advised that any form of cyber abuse against the school or another member of the school community is not tolerated. Any incidents of cyber abuse/bullying should be reported to the Principals/Deputy Principal and will be subject to sanctions as outlined below.

Users will not type, record or reproduce obscene, profane, lewd, vulgar, rude inflammatory, racist, homophobic, threatening or disrespectful language, images, audio or video. Information which could cause damage or disruption may not be posted. This includes inside of school and outside of school hours relating to school.

Users will not knowingly or recklessly post fake, declamatory or slanderous information about any person, group or organisation. Users will not engage in defamatory, slanderous, prejudicial or discriminatory comments, to distress, annoy or attack another person.

Should Users cause damage to the ICT systems, they are required to bear the cost of repair or replacement of said system.

Users will not publish on behalf of Ardscoil Rath Iomgháin, Rathangan.

The school reserves the right to review, audit, intercept, access and disclose all messages created, received or sent for any purpose.

Care must be taken that all documents and computer media are disposed of securely at the end of their life, shredded or given to the ICT Service Team for secure digital disposal.

5. Data Storage

Users should store all files on the schools servers in the users assigned Home Folder unless otherwise instructed.

If any sensitive data such as student records including but not limited to disciplinary action, grades, home addresses and contact details need to be taken off premises including transmission over the internet by e.g. email then this information should be encrypted. Encrypted storage devices can be purchased from the ICT Support Team.

The school servers are automatically backed up during regular intervals using best practice and in accordance with relevant legislation.

6. Adherence and Sanctions

IT is mandatory that all staff, students, volunteers and other users of Ardscoil Rath Iomgháin adhere to this Information and Communications Technology Acceptable Usage Policy.
Any breach of this policy is regarded as a serious offence. Offenders shall be liable for disciplinary actions including possible termination of services, suspension, dismissal/expulsion and or civil and/or criminal charges in line with the schools code of behaviour and/or local, European and international law.

All users of Ardscoil Rath Iomgháin's ICT Systems and services are required to sign the attached acceptance form before ICT access is provided.

I _____(full name) hereby certify that I have read and understand my rights and responsibilities while using the ICT systems and services provided to me by Ardscoil Rath Iomgháin and its partners as outlined in the Schools ICT Acceptable usage policy.

I agree to abide by the rules and responsibilities set out in the schools ICT Acceptable usage policy and will accept any disciplinary actions deemed appropriate, if I am proven to be in breach of this policy.

Signature: _____ Date:__ __/____ /__ __ __ __

Year _____ Class _____

Parents/Guardians

I_____as the parent or legal guardian of the above student hereby certify that I have read and understand the schools ICT Acceptable usage policy; I understand that the schools computer systems and services are intended for educational purposes. I also understand that every reasonable precaution has been taken by the school to provide online safety and the school cannot be held responsible if students access unsuitable websites.

Signature :_____ Date:__ __/____ /__ __ __ __

Address: _____ Telephone:_____