Acceptable Use of Information and Communications Technology Policy

2020

Mission Statement

Ramsgrange Community School is a welcoming, open and inclusive school. Our aim is to develop each of our students as a whole person by promoting an atmosphere of respect, honesty and fairness in which all of the school community can achieve their full potential.

RCS Vision: Respect, Community, Success

Rationale:

Our Students engage confidently with Information and Communications Technology (ICT) in their social and recreational lives. ICT integration in the classroom can be a hugely positive addition to the learning environment. ICT can bring rich and varied learning resources into the classroom which can lead to the creation of a more dynamic, rewarding and productive learning environment. ICT, in whatever form, should be considered as a tool which can assist and support the delivery of the curriculum.

The aim of this Acceptable Use Policy (AUP) is to ensure that pupils will benefit from learning opportunities offered by the school's Internet resources and mobile phones in a safe and effective manner. Internet use and access is considered a school resource and privilege. Teachers will also be mindful when assigning homework that all students may not have access to resources such as mobile phone and internet access at home. Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions - as outlined in the AUP - will be imposed.

*Users refer to students, teachers, administrative staff, other members of school staff and visitors using the school facilities.

This policy should be read in conjunction with our Blended/Online Guidelines Booklet (available on school website) when the school is in a mandated lockdown.

What is ICT?

ICT (information and communications technology - or technologies) is an umbrella term that includes any communication device or application, encompassing: radio, television, mobile phones, computer and network hardware and software, satellite systems and so on, as well as the various services and applications associated with them, such as videoconferencing and distance learning.

Digital Rights and Responsibilities:

The definition of digital rights and responsibilities is having the right and freedom to use various types of digital technology while using the technology in an acceptable and appropriate manner.

Other school policies:

The following is a list of school policies, practices and activities that are particularly relevant to AUP

- Mission Statement
- Anti-Bullying
- The School Care Team
- Extra-curricular activity
- Code of Behaviour
- Class Tutor system
- Major Incidents procedures

The Board has ensured that the necessary policies, protocols or practices as appropriate are in place in respect of each of the above listed items.

Acceptable Use – Guidelines and Procedures:

1. When using the Internet, all school staff (both teachers and support staff) must comply with all copyright, libel, fraud, discrimination and obscenity laws, and all school staff are expected to communicate in a professional manner consistent with the rules of behaviour governing employees in the Education Sector and Teaching Council Code of Conduct.

Staff & Students should ensure that students know and understand that **no** Internet user is permitted to:

- Retrieve, modify the security settings/configuration of the school's PC and IT facilities, send, copy or display offensive messages or pictures;
- Use obscene or racist language;
- Harass, insult or attack others;
- Damage computers, computer systems or computer networks;
- Violate copyright laws;
- Use another user's password;
- Trespass in another user's folders, work or files;
- Intentionally waste resources (such as on-line time and consumables);
- Use the network for unapproved commercial purposes.
- Use a VPN (even on a personal device). These must be disabled upon logging onto the school network.
- When using school issued Microsoft licenses, users must be aware that normal school rules apply as if being used in the classroom, even when out if school hours. Teams, Outlook, etc. are not for private use.
- When using video conferencing software, students are asked to leave mic and camera ON unless instructed to do otherwise.
- Students will only use approved school email accounts or licensed platforms to contact staff members
- Uploading and downloading on school computers is expressly forbidden.
- School administrators reserve the right to regularly monitor students school issued licenses.
- Students will continue to own the copyright on work sent via school licensed apps.

Students are responsible for their own IT equipment; these items are not covered by the school's insurance.

2. **Location and Supervision**

It is an absolute requirement that the school ensures that access to the Internet provided to staff and students is a filtered service. The filtering service is provided by N.C.T.E. The school management reserves the right to review such access and revoke Internet access. Staff are informed that the I.C.T. system in the school records websites visited.

Internet access for students will be available only on computers/mobile phones that are in areas of the school such as classrooms, libraries, study rooms, computer laboratories or where permission is granted by the Teacher. Machines, which are connected to the Internet, must be in full view of people circulating in the area.

3. **Internet & Mobile Phones as a Teaching Resource**

Our School supports the use of teachers' resources in their teaching and learning activities, to conduct research, and for contact with others in the education world.

Staff are encouraged to investigate the possibilities provided by access to this electronic information and communication resource, and blend its use, as appropriate, within the curriculum.

The use of ICT, including mobile phones, is solely at the discretion of the teacher. Any breach of such privileges will result in withdrawal of same.

The use of mobile phones is not allowed at break times.

When being used in class the phone should be **placed camera side down on the desk**.

Examples of Acceptable and Unacceptable Use of the I.C.T. facilities available to staff in Ramsgrange Community School:

a. On-line activities which are **encouraged** include:

- use of email and computer conferencing for communication between colleagues, between students(s) and teacher(s), between student(s) and student(s), between schools and industry;
- use of the Internet to investigate and research school subjects, cross-curricular themes and topics related to social and personal development;
- use of the Internet to investigate careers and further and higher education;
- development of students' competence in ICT skills and their general research skills.
- Use of mobile phone cameras for research and documentation purposes
- Use of appropriate educational APPs

b. On-line activities which are **not permitted** include:

- visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material;
- downloading text or images which contain material of a pornographic, racist or extreme political nature, or which incites violence, hatred or any illegal activity;
- using the computer to perpetrate any form of fraud, or software, film or music piracy;
- using the internet to send offensive or harassing material to other users;
- downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence;
- hacking or accessing unauthorised areas;
- publishing defamatory and/or knowingly false material about Ramsgrange Community School, your colleagues and/or our students on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format;
- revealing confidential information about Ramsgrange Community School in a personal online posting, upload or transmission - including personal information and information relating to our students, staff and/or internal discussions;
- undertaking deliberate activities that waste staff effort or networked resources;
- introducing any form of malicious software into the school network;
- searching, viewing and/or retrieving materials that are not related to the aims of the curriculum or careers information that is relevant to students;
- copying, saving and/or redistributing copyright protected material, without approval;
- subscribing to any services or ordering any goods or services, unless specifically approved by the Principal;
- playing computer games or using other interactive 'chat' sites;
- publishing, sharing or distributing any personal information about any member of staff without their permission (such as: home address; email address; phone number, etc.)

Any breach of this Internet Acceptable Use Policy may lead to disciplinary action as outlined in the Code of Behaviour. All staff (teachers, student teachers, SNAs, ancillary staff) that use the school's internet service is required to sign this agreement confirming their understanding and acceptance of this policy.

Guidelines for Students for blended learning

Each student in the school has/will be given licences to a full suite of Microsoft apps. These will be essential for distance learning. Students will use their allocated login to gain access to these apps. Among the most important apps are:

- **Microsoft Word** - This is a word processing app which will enable students to create pages of writing - https://www.youtube.com/watch?v=HC13M8FGlNc
- **Microsoft PowerPoint** - This is a app where students can create presentations using word processing as well as audio/visual elements – https://www.youtube.com/watch?v=u7Tku3_RGPs
- **Microsoft Outlook** - This is an email app where students can contact/be contacted by members of staff as well as other students – https://www.youtube.com/watch?v=WfSCfBntqPU
- **Microsoft Teams** – This app allows staff to put students into class groups to allocate work and even video call/message - https://www.youtube.com/watch?v=bAesIjrem7E&list=PLmkaw6oRnRv8UYcRLpxon4rPQm_pud8nd&index=16
- **Microsoft SharePoint** – This is an online resource bank where teachers and students can share files online using cloud technology. This is very useful as larger files such as movie clips and whole subject presentations can be stored here - https://www.youtube.com/watch?v=odixpcyqOgQ
- **Zoom** – Video conferencing app where lessons can be taught - https://www.youtube.com/watch?v=QOUwumKCW7M

All activity on the Internet is monitored and logged.

Sanctions for breach of Policy as per Code of Behaviour 2018

In the event of the non-co-operation of a student, the following procedures apply:

Reason with the student while making sure that they understand the consequences of their actions for everyone involved. A restorative conversation will be had with the student so they understand the consequences of their actions and take responsibility for their behaviour.

In the event of negative behaviour occurring in class, subject teachers have a range of sanctions available to them.

These include:

- Verbal reprimand
- Moving the pupil to a different location within the class
- Assigning extra work
- Issue Incident Report to Yearhead on Vsware
- Possible referral for counselling session by Yearhead/ SST
- Note sent to parents in Student Journal and record of the behaviour on Vsware (Negative point/ Serious breach)
- Referral to Deputy Principal in the case of gross misbehaviour.

This list is not exhaustive (please see COB for other examples of sanctions).

In the event of an incident occurring, which, in the view of the class teacher is of sufficient severity to require further sanctioning, the matter must be referred to the relevant Year Head or Deputy Principal. Any sign of sustained improvement needs to be met with approval.

ICT and Legislation - the following legislation is relevant to Internet Safety.

1. Data Protection Act 1998 - this act was passed in order to deal with privacy issues arising from the increasing amount of information kept on a computer about individuals.
2. Data Protection (Amendment) Act 2003 - this amendment extends the data protection rules to manually held records and also makes improvements to the public's right to access data.
3. Child Trafficking and Pornography Act 1998 - this act legislates against anyone who knowingly produces, prints, publishes, distributes, exports, imports, shows, possesses or sells child pornography.
4. Interception Act 1993 – this act stipulates that telecommunication messages can be intercepted for the purpose of an investigation of a serious offence. Authorisations are subject to certain conditions.
5. Video Recordings Act 1989 - this act prohibits the distribution of videos which contain obscene or indecent material which may lead to the depravation or corruption of the viewer.
6. Copyright and Related Rights Act 2000 – this act governs copyright in Ireland.

This policy will be reviewed by the BOM when necessary