Acceptable Usage Policy

January 2017

Skerries Community College

Any breach of this ICT Acceptable Usage Policy may lead to disciplinary action. All staff (teachers, student teachers, SNAs, ancillary staff) and students who use the school's IT equipment and internet service are required to sign this agreement confirming their understanding and acceptance of this policy

INTRODUCTION

IT and the Internet are rich and valuable sources of information and have a very important part to play in the education of students. However, coupled with these opportunities there are risks involved in the use of IT and the Internet. In order to minimise these risks the use of IT and the Internet at Skerries Community College are governed by this policy.

MISSION STATEMENT

Skerries Community College promotes the development of the whole person within the Christian context. With the assistance of parents we aim to develop responsible citizens. Students, irrespective of economic circumstance, gender, religious or philosophical outlook, race or social situation are welcome to join us in the pursuit of knowledge. Our ethos is based on personal responsibility, independence, respect for people and the respect for property. Our school seeks to cultivate integrity, the necessary skills for life, and valuing discipline and punctuality, to facilitate the best in the academic and non-academic areas. We value our culture, our traditions, our heritage and we seek to be a caring and compassionate community where justice and truth are central elements.

RATIONALE

The Acceptable Use Policy is a series of documents, which addresses all rights, privileges, responsibilities and sanctions associated with access to, and use of, IT and the Internet in Skerries Community College. The aim of this Acceptable Use Policy is to ensure that pupils will benefit from learning opportunities offered by the College's Internet resources in a safe and effective manner. While there are many overlaps the policy differentiates between the requirements for staff and those for pupils.

SCOPE

This policy has been designed to protect the students and all staff members of Skerries Community College. This policy links to and draws upon our other policies including the Child Protection Policy, Anti-bullying Policy, Homework Policy, Dignity in the Workplace Policy, Health and Safety Policy, Mobile Phones Policy and Code of Behaviour. Any breaches of this Policy will be dealt with as a College / DDLETB Discipline Issue.

Technologies Covered: Skerries Community College may provide students with internet access, computers, digital imaging equipment, including Laser Technology, 3D printing and CNC equipment, laptop or tablet devices, video-conferencing capabilities, virtual learning environments, online collaboration capabilities, online discussion forums, email and more. As new technologies emerge SCC my provide access to them also.

The policies outlined in this document are intended to cover all online technologies used in the school, not just those specifically mentioned.

SCC provides students with email accounts for the purpose of school-related communication. Email accounts should be used with care and may be monitored and archived.

Students are expected to communicate with the same appropriate, safe, mindful and courteous conduct online as offline.

Student email accounts (@skerriescc.com) may be subject to inspection at any time

SCC's mobile devices:
SCC may provide students with mobile computers, digital recorders or other devices to promote learning. Students are expected to treat these devices with respect. Students may not alter/load any software on these devices. They should report any loss, damage or malfunction to their teacher or the relevant staff member immediately. Students may be financially accountable for any damage resulting from negligence or misuse.

Students may use personally owned devices (eg. laptops, digital cameras, phones) for educational purposes only if allowed by their classroom teacher on each and every occasion. Appropriate online behaviour and adherence to the acceptable usage policy should always be used. Students are reminded that digital recording of any member of the school community without their express and direct permission is an offence in law.

SCC Security
Teachers / Students are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programmes and not opening files or programmes of unknown or untrusted origin.
Use common sense. Inform your teacher or the relevant staff member immediately. Think twice before you click on anything you feel is not right.
If you believe a computer or mobile device you are using might be infected with a virus, please alert your teacher or the relevant staff member.
For the security of our network and the safety of our students no student should download any file onto the College's mobile devices without the direct permission of and instruction from their teacher or the relevant staff member.
Students/ Teachers should also recognise that along with the valuable content online there is unverified, incorrect or inappropriate content. Students / Teachers should use trusted sources when conduction research via the Internet
Students should not post anything online that they wouldn't want parents, teachers or future colleges or employers to see.

Personal Safety:
If you see a message, comment, image or anything else online that makes you concerned for your personal safety, bring it to the immediate attention of

- a teacher if you are at school
- a parent / guardian if you are at home
- Relevant staff member

Students should never share personal information about themselves or others, including phone numbers, addresses, PPS numbers, dates of birth over the internet without adult permission
Students should never agree to meet someone they meet online in real life without parental permission. Be aware that it is almost impossible to verify the real / true identity of an on-line correspondent.

Cyber-bullying:

Cyber bullying is covered under the College Anti-Bullying Policy. Harassing, flaming, denigrating, fraping, impersonating, setting up a false account, outing, tricking, excluding and cyber-stalking are all examples of cyber bullying. In addition the following should be noted:

- Such bullying will not be tolerated in SCC
- Do not send emails or post comments or photos with the intention of scaring, hurting, or intimidating someone else, even as a joke.
- Engaging in any online activities intended to harm (physically, emotionally, reputationally) another person , will result in severe disciplinary action.
- Harassment is a crime and cyber-bullying is considered to be harassment
- Remember that your activities are monitored, retained and can be traced.

Assistive Technology

Assistive Technology (AT) is covered under the college's AT Policy.

Section A: Staff

CONTENT

The College is responsible for safeguarding children and it is important that all staff take all possible and necessary measures to protect children in their IT usage in school and to encourage them to be safe whilst using the Internet for any College related matters.

Staff must endeavour to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff (teachers, student teachers, SNAs, ancillary staff) are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

1. Skerries Community College supports and encourages the use by teachers of a wide range of resources in their teaching and learning activities, the conducting of research, and 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. It is expected that over time explicit reference will be made in Subject Department Plans to the ICT resources and websites that are used in the teaching and learning.

2. When using IT and the Internet, all school staff (both teachers and support staff) must comply with all copyright, libel, fraud, discrimination and obscenity laws. All school staff are expected to communicate in a professional manner consistent with

the rules of behaviour governing employees in the Education Sector and with the Teaching Council Code of Conduct.

3. Staff should be aware of the risks of breaking confidentiality and Data Protection laws by giving students or other parties access to their teacher logon accounts.

Staff should know and understand that **no** user of IT / Internet is permitted to:

- *retrieve, modify the security settings/configuration of the school's PC and IT facilities, send, copy or display offensive messages, images or pictures;*
- *use obscene, homophobic, misogynistic or racist language;*
- *use IT to harass, insult or attack others;*
- *damage computers, computer systems or computer networks;*
- *deliberately violate copyright laws;*
- *use another user's password or account*
- *trespass in another user's folders, work or files;*
- *use the network for unapproved commercial purposes.*

4. 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 DDLETB and PDST. The school management reserves the right to review such access and revoke Internet access. *Staff should note that the I.C.T. system in the school has the capacity to record websites visited.*

5. It should be noted that;

- when students are accessing computers they must under the supervision of a teacher and that access to the computer room, outside of the timetabled schedule is via the booking form in the Staffroom and such access must be supervised.
- if students' work is uploaded to any site it must be in an educational context and have a copyright notice prohibiting the copying of such work without the expressed written permission of the owner of the work.
- any audio, video or photographic clips uploaded to the College's website will focus on group activities and will, where feasible, avoid the direct identification of students by full name – first and surname.
- it is not advisable for staff to send personal emails or text messages to any student.

6. Skerries Community College would like staff members to note that the following activities are not permitted:

- visiting or encouraging others to visit or publicise internet sites that contain obscene, hateful, pornographic or otherwise illegal material;
- downloading text or images which contain material of a pornographic, racist or extreme nature, or which incites violence, hatred or any illegal activity;
- using IT or the Internet to perpetrate any form of fraud, or software, film or music piracy;
- using IT or the internet to send offensive or harassing material to other users or links to such sites;
- 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 or agreement;
- hacking or accessing unauthorised areas;
- publishing defamatory and/or knowingly false material about Skerries Community College, our colleagues and/or our students on the school system / network, social networking sites, blogs online journals, 'wikis' and any online publishing format;
- revealing confidential information about Skerries Community College in a personal online posting, upload or transmission - including personal information and information relating to our students, staff and/or internal discussions and school business;
- undertaking deliberate activities that waste staff effort or network resources;
- introducing any form of malicious software into the school network;
- consciously searching, viewing and/or retrieving materials that are not related to the aims of the curriculum, education 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 where the school will be billed unless specifically approved by the Principal;
- playing computer games or using interactive chat sites that are unrelated to education;
- publishing, sharing or distributing any personal information about any member of the College community – student or staff member, without their permission (such as: home address; email address; phone number, etc.)

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law. Please sign below if you agree to the above conditions.

Section B: Students

All students have a responsibility to use the school's IT and computer system in a lawful and ethical manner. To ensure that students are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

1. When using the Internet, all students must comply with all copyright, libel, fraud, discrimination and obscenity laws.

- No student is allowed access to computers without the permission of a teacher and will, where possible, be supervised by a teacher
- All users will observe good IT practice at all times and will not undertake any action that may bring the College into disrepute.
- Filtering software will be used in order to minimise the risk of exposure to inappropriate material. Students must not attempt to bypass the filtering software.
- The College may regularly monitor pupils' internet usage.
- Uploading and downloading of non-approved software, photos, music, files etc. is not permitted.
- The use of personal USB sticks, DVDs, or other data storage devices is prohibited**.**
- Internet usage may be monitored and recorded for security and / or network management reasons. This includes students' 365 emails.

2. Students should know and understand that **no** IT/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, images or pictures;*
    - *use obscene, homophobic, misogynistic or racist language;*
    - *use IT to harass, insult or attack others;*
    - *damage computers, computer systems or computer networks;*
    - *violate copyright laws;*
    - *use another user's password, logon account with or without their express permission*
    - *trespass in another user's folders, work or files;*
    - *use the network for unapproved commercial purposes.*
    - *Save any inappropriate data on school network*
    - *Load any software on school computers.*
    - *Bypass any school computer /network settings.*

3. Skerries Community College wish to inform students that the following activities are not permitted:

    - visiting internet sites that contain obscene material;
    - Uploading, downloading or viewing text or images which contain material of a hateful, pornographic, racist or otherwise illegal nature, or which incites violence, hatred or any illegal activity;
    - playing computer games or using interactive 'chat' sites that are unconnected to education;
    - using IT for software, film or music piracy;
    - using IT to send hurtful, bullying or harassing material to other users or links to such sites;
    - downloading copyrighted materials belonging to other people (ie. plagiarism)
    - hacking or accessing unauthorised areas;
    - publishing damaging and/or knowingly false material about Skerries Community College, or any member of the College community on social networking sites, blogs, tweets or any online publishing format;
    - revealing private information about Skerries Community College in a personal online posting, upload or transmission - including personal information and information relating to our students, staff or school business;
    - undertaking deliberate activities that waste staff effort or networked resources or the sharing of teachers' or students' work, notes etc. with those who are not part of the College community.
    - introducing any form of malicious software into the school network;
    - searching, viewing and/or accessing materials that are not related to school work
    - copying, saving and/or redistributing copyright protected material, without approval;
    - publishing, sharing or distributing any personal information about any member of the College community – student or staff member, without their permission (such as: home address; email address; phone number, etc.)

Parents must ensure that their children fully understand this Acceptable Usage Policy

This is not an exhaustive list and all students are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law. Please sign below if you agree to the above conditions.