The Clere School

Student IT Acceptable Usage Policy

Date of Policy Issue: September 2023
Approved at Whole Governing Body on: September 2023
Due for Review: September 2024
Statutory/Discretionary: Discretionary
Policy Responsible: Business Manager

The Clere School, henceforth referred to as 'the school', envisages and actively develops an environment where the use of Information and Communication Technology (IT) is regarded as an integral part of our everyday teaching and learning practices and administration management. We recognise that IT has the potential to significantly impact learning outcomes for all students and the work habits of all staff by making them more independent and collaborative members of the school's learning community.

Contents

1. Introduction
2. User responsibilities
3. Access to computers outside of lessons
4. Leisure use / work use
5. Equipment
6. User names and passwords
7. Software, copyright and privacy
8. Printing
9. Sanctions

1. Introduction

The purpose of this policy is: -

- To inform all students of the school's IT equipment and infrastructure and what constitutes appropriate and safe use.
- To outline the eSafety rules for all users of the school IT network.

All staff and students at the school are provided with access to IT facilities for work and communication across the school site. Only teaching and support staff have access to the administrative applications such as SIMS and this is on a least privilege required basis set by the Business Manager in consultation with the Headteacher. All systems and usage are monitored by the IT Support Assistant alongside the IT Support Team.

The school expects individuals to be careful, honest, responsible and civil in the use of IT equipment on the network. The IT resources should be used for purposes related to the school's vision and policies of teaching and learning.

The school network comprises of the following: -

- Hard wired Desktop Computers across the site.
- Servers and backup facilities.
- Laptops (student and staff) and any associated trollies
- Wireless access points across the school site.
- Wired Network infrastructure.
- Printers and scanners.
- Apple Mac Suite.
- Digital cameras and DV cameras.
- CD-ROMS, DVDs and Flash Drives.
- All audio-visual equipment around the school including digital projectors, audio systems and interactive whiteboards.

2. User responsibilities

1. The school owns and maintains the entire network and IT equipment onsite and information stored on the school network remains the property of the school.
2. Use of any of school owned computer or network equipment for private, commercial, non-school business purposes without explicit authorisation is prohibited and will result in the termination of network privileges. All users must recognise that computers and networks are limited resources; users must use them efficiently and with respect.
3. Students are discouraged from bringing expensive and personal electronic equipment onsite, but the school recognises the ubiquitous nature of mobile phones, iPods etc. They must always be kept out of site whilst in the school, in line with other school policies.
4. Students should use the school's Office365 service to communicate, ensuring all messages will be written carefully and politely, particularly as e-mail could be forwarded to unintended readers.
5. Social networking sites are an inevitable part of many students' everyday lives. It is recognised that for many these sites are used in a proper and respectful manner. When a student uses these sites to post information that is offensive, harmful, libellous or otherwise

inappropriate towards any member of the school community the matter will be taken very seriously. The school will follow the discipline/behaviour policy and the individual will be put at risk of exclusion.

6. No student should use social network sites, such as Facebook or Twitter at school, and they will not have school staff as friends on such a site.
7. The sending of anonymous messages, chain letters and the use of mobile phones to take photos of staff and students without their permission is not permitted.
8. Students must take care not to reveal personal information through email, personal publishing, blogs, twitter, texts or instant messaging.
9. Individuals assume personal responsibility for the use of their network accounts. Consequently, users must not disclose their passwords to other individuals (including family or friends). The possession or collection of passwords and usernames belonging to other users is prohibited.
10. Users may not copy, publish, store or transmit data if when doing so would constitute a violation of copyright or data protection act.
11. Users are prohibited from installing, storing or using any software on the school network not approved/managed by the IT Support Team. Transmission of such software across the network is also prohibited.
12. The introduction of data or programs which in some way endangers computing resources or the information of other users (e.g., a computer worm, virus, or other destructive program), or which infringes upon the rights of other school users (e.g., inappropriate, obscene, pornographic, bigoted, racist or abusive materials) is strictly prohibited.
13. Students must report any damage to the IT system immediately. Any person caught damaging any IT equipment will be prohibited from using the facilities for a period, their parents will be sent an invoice for the repair or replacement of damaged equipment and further sanctions may be enforced according to the school's Behaviour Policy.

3. Access to computers outside of lessons

The library is the main place for students to work outside of lessons. In addition, three dedicated computer rooms (IT1, IT2 and DT2) can be used at lunchtimes and after school when supervision is available.

All three rooms may be used during lesson time if the room is free and supervised by a member of staff.

There are computers in many other parts of the school, and these may be used with the permission of your teacher, only for work related to the set curriculum.

4. Leisure use / work use

The priority of use is always given to students who wish to complete schoolwork. It is recognised that students want to explore the use of computers and that this is generally for their own interest and therefore a leisure activity.

If a student from any year group needs to do schoolwork, they may request that a student using the computer for leisure activities logs off and leaves the computer.

5. Equipment

Students are not allowed to alter the setup of any IT equipment. For example: -

- Students must not unplug items such as monitors, keyboards, mice etc.
- Students must not change any monitor settings.

6. User names and passwords

- It is essential that students keep their password secret. A student is held responsible for all activities that are undertaken using their username and password. Students should ensure that when logging on no one is looking at the keyboard whilst they type in their password.
- It is forbidden to use another student's username to log-on.
- Collaboration such as peer assessment and group work are done electronically via Microsoft Teams.

7. Software, copyright and privacy

- Students may only use software that the school has installed for their use. Students are not permitted to install or run software which they have brought into school on a Flash disk or which has been downloaded from the Internet.
- When copying a picture or a quotation from the Internet or any other information source, the source must be cited in the student's work. Any words copied must be in quotation marks, so the words are not the student's own words. In general, it is better for students to write their own words, using electronic sources for diagrams only. All sources must be cited.
- The IT Support Team may at any time view materials that a student has on a school computer to ensure that the equipment is being used responsibly. The materials stored on the network are the property of the school.
- School computers must not be used for financial gain, political activity or advertising.

8. Printing

- All students and staff have access to a range of school printers (B/W and Colour) and these should be used sparingly. All users should check their documents using Print Preview first to eliminate errors before printing.
- Students should avoid printing documents with a solid colour background since these are extremely expensive.
- Students may only print multiple copies of the same document with permission from a member of IT staff. General practice is to allow single prints only.

9. Sanctions

Acceptable use is everyone's responsibility and we expect all students to use the equipment responsibly in order for themselves and others to have the right to use the IT equipment for learning.

In the case where misuse and abuse get discovered the following sanctions will be enforced:

LEVEL 1 VIOLATION Unauthorised access to computer material

This includes, for example, finding or guessing someone's password, then using that to get into a computer system and have a look at the data it contains. This is an offence even if no damage is done, and no files deleted or changed. The very act of accessing materials without authorisation is illegal and is therefore strictly prohibited at the school.

SANCTION: Suspension of account, detention.

LEVEL 2 VIOLATION Unauthorised modification of computer material

This could include deleting files, changing the desktop set-up or introducing viruses with the intent to impair the operation of a computer, or access to programs and data. This comes under "The Computer Misuse Act 1990" clearly and is viewed as hacking

SANCTION: Suspension of account, parents informed, possible exclusion.

LEVEL 3 VIOLATION Intentional damage to equipment

This could include removal of keys, piercing a TFT screen, graffiti or removal/stealing of computer equipment.

SANCTION: Isolation from use of IT equipment for a length of time, invoice for cost of equipment, parents informed and possible exclusion.

Depending on the seriousness of the offence, internal sanctions might range from first warnings to temporary bans from using IT resources, to involvement of parents and in extreme cases temporary/permanent exclusion.

Most offences are likely to be students simply playing around, to see what they can do. However, if something more serious is suspected for example, using the school's computers to gain unauthorised access to other computers outside the school, then it may be necessary to involve the police and we will not hesitate to take this route.