St David's
Coleg Catholig Dewi Sant
Catholic Sixth Form College

IT Policy – User Systems

IT Policies for staff and student facing systems:
Student Acceptable Use

Author	Jon Carolan
Issue Date	21/04/2019
Equality Impact Assessment	Y
Status	Approved
Approved by	Governing Body
Approval date	20/4/2019
Review date	20/4/2022

1. Introduction

The availability of IT facilities to all members of the College is central to the proper functioning of the College.

Misuse is regarded as a matter of utmost seriousness. Evidence of persistent misuse will be pursued under disciplinary rules. Evidence of theft or malicious damage, or attempted unauthorised access may result in legal proceedings.

This document outlines the expectations placed on all users of IT systems of the College.

2. Approach

The underlying philosophy is that the College's computing facilities should be used in a manner which is ethical, legal and appropriate to the College's aims. IT facilities must be used in a manner which does not obstruct the work of others and which encourages a scholarly atmosphere to be maintained. The system is a shared resource and each user has responsibility to learn how to use it appropriately. The College encourages the use and exploration of its IT system but discourages behaviour which may inconvenience other users.

IT facilities includes all computer systems and computing hardware, software and networks made available by the College.

3 Scope

This policy applies to all users of IT facilities in relation to:

- the use of computing devices;
- IT facilities owned, leased, hired or otherwise provided by the College, connected directly or remotely to the College's network or IT facilities or used on the institution's premises, or individuals connecting their equipment to the network i.e. personal laptops.
- cloud-based services such as Office 365, Moodle and remotely hosted systems

4 Access to and the Use of IT Facilities

No-one may use IT facilities without prior registration.
Registration to use the College's IT facilities constitutes acceptance of this policy.

Users are given access to those parts of the system which are appropriate to their role. Users are therefore not normally expected to seek access to other parts of the system unless authority is given. Unauthorised access to data is not acceptable and may result in disciplinary action.

The granting of access rights to IT facilities will be by the provision of access cards, user IDs and passwords giving access to locations, hardware and/or software facilities. The provision of such user references and passwords will constitute access rights for the use of those IT facilities under the conditions applicable to those facilities.

Users of IT facilities are expected to comply with the conditions of use which include the following. Users must not:

- disclose user ids, personal passwords which give access to the system (NB personal passwords should be changed regularly)

- enable unauthorised third party access to the system
- deliberately damage IT equipment
- delete, amend or otherwise corrupt the data or data structures of other users without their explicit permission
- knowingly introduce viruses or other harmful programmes or files
- connect to any internal IT facility without the permission of the appropriate manager
- attempt to gain deliberate unauthorised access to external facilities or services
- use the IT facilities to send unsolicited, unauthorised commercial or illegal advertising or other material
- load software for which no licence is held
- modify software
- use the IT facilities of the College for commercial gain without the explicit permission of the appropriate authority.

Much of the information held on the College's IT system is confidential and must not be disclosed to other parties.

The College expires passwords when they have not been changed for 90 days, which may occur during holidays depending on when the password was last changed. The passwords must meet set criteria in terms of complexity and length details of which can be obtained from the IT Support. The College provides facilities for users to reset passwords remotely, which require registration before use. **It is not possible to reset passwords via telephone or e-Mail from an unregistered address.**

The College regularly carries out scheduled backups of the IT systems in accordance with the Backup Policy. This is done with disaster recovery in mind so in the event of hardware failure or external problems that systems can be recovered in a reasonable amount of time. Although user areas are included in this process, this does not mean that the College is responsible in the event of loss resulting in data being irretrievable. **Users are responsible for their own work and should regularly take their own independent backup of their user areas or cloud-connected storage.**

The Data Protection Act 1998 outlines the legal position in relation to the use of data. Users who would like advice about the content or implications of this Act should contact the Data Protection Officer via HR.

Access to Office 365 is provided for the purpose of storing work and for e-Mail, as well as other tools. Access to this system is provided automatically while a valid account exists on the College network. The College cannot be held responsible for issues arising as a result of the inability to access this system as a result of forgotten passwords, withdrawal of account as a result of misuse, or for the content of information stored within the Office 365 system.

The college reserves the right to access any data stored within any facility provided as a user. This includes but is not limited to user and shared network storage, Office 365 e-Mail and OneDrive /Sharepoint storage as well as transmission or access logs such as web or other audit logging facilities. Action may be taken against individuals who in the opinion of the College have breached any policies whether IT-related or not.

5 Equipment

Users are responsible for ensuring that they are sufficiently familiar with the operation of any equipment they use to make their use safe and effective.

No equipment or other IT facility may be moved without the prior agreement of IT Support.

Serious damage or the theft of IT equipment should be reported to a member of staff who will advise the necessary departments.

Students are not to connect their own equipment to the physical or wireless network without the approval of the IT Manager, expect for the Eduroam and Guest networks provided for this purpose.

6 The Use of E-Mail

The use of electronic mail (e-mail) has grown significantly to the extent that it now represents an important means of communication both inside and outside of the College. The e-mail system can be accessed by all users whose role and responsibilities require them to use the computer network. Its use is therefore extensive and hence it is important that all of its users recognise that, whilst such a system can have many benefits, there are also limitations.

Users should note that e-mail is considered by the College as a standard communication mechanism. Those student who are given access to the system will therefore be expected to access the facility as regularly as necessary to send and receive information.

E-mail is a fast and convenient means of communicating information. However because of this there may be a temptation not to take sufficient care when initiating messages and sending replies. It is important that users recognise the need to pay the same care and attention to the composition of e-mail messages as to other forms of written communication. Care should be exercised in constructing messages, for example, the use of capitals is considered to be the equivalent of shouting. E-mail lacks the cues and clues that convey the sense in which what you say is to be taken, and the wrong impression can easily be conveyed.

E-mail is a valuable means of communication and can be the most appropriate mechanism in a variety of circumstances for example, for short memos, when the purpose of the communication is to convey straightforward information, where speed of communication is important and where a consistent message to a number of people is required. However there are also a number of situations where it is unlikely to be the most appropriate, for example

- when the information to be communicated is complex and/or lengthy
- when discussion about a topic is likely to be necessary and hence face to face contact is more appropriate
- when a signature is required on a communication.

E-mail should not be used as a means of storing important information.

Email is provided for College use only – it is not to be used for managing personal matters or social media accounts.

Although there a systems put in place to prevent SPAM, Phishing or other malicious emails, occasionally some will come through. If you believe that you have received an email of this type, do not click on any links or attachments and contact IT Support.

7 Unacceptable Behaviour

Unacceptable behaviour in relation to the use of IT systems will not be tolerated and where it is identified there are a range of informal and formal routes which may be followed including disciplinary action where necessary.

Some forms of behaviour will always be considered to fall below the standard of acceptability. These include:

- the use of inappropriate language in communications;
- sending inappropriate messages including those which are discriminatory, sexually harassing or offensive to others on the grounds of race, disability, gender, religion or sexual orientation;
- the sending of potentially defamatory messages which criticise other individuals or organisations (legally e-mail is classified as a form of publication, governed by the rules of disclosure, libel and employment law);
- the creation, display, production, circulation or transmission in any form or medium of inappropriate material, such as pornographic or other offensive material from the internet;
- forwarding confidential, sensitive or personal information onto third parties without gaining appropriate consent;
- using the IT system for commercial gain;
- overloading the system by sending inappropriate bulk messages;
- sending messages which are rude, overbearing, aggressive or bullying.

Users have a responsibility to ensure that copyright and licensing laws are not breached when composing or forwarding e-mails, e-mail attachments and using the internet. The laws regarding breach of copyright apply equally to the downloading and copying of information from the Internet. Users must be clear whether there is an entitlement to download information before using and disseminating this.

8 Safeguarding & IT Users

Safeguarding of learners is an integral part of the acceptable users policy. As part of this policy, St David's Catholic College will:

• Promote and prioritise e-safety for all members;
• Establish an understanding of roles and responsibilities in respect of e-safety and ensure everyone is provided with appropriate learning opportunities to recognise, identify and respond to any concerns regarding to the use of internet technologies and other electronic communications;
• Ensure that appropriate action is taken in the event of any e-safety concerns and support is provides to the individual(s) who raise or disclose the concern;
• Ensure that confidential, detailed and accurate records of all e-safety concerns are maintained and securely stored;
• Ensure that robust e-safety arrangements and AUPs are in operation;

Roles and Responsibilities

The College IT Manager will ensure that:

1. Staff members receive the appropriate training, guidance, time and resources to effectively implement online safety policies and procedures.
2. Clear and rigorous policies and procedures are applied to the use/non-use of personal ICT equipment by all individuals who come into contact with the setting. Such policies and procedures should include the personal use of work related resources.
3. The Acceptable Users Policy is implemented, monitored and reviewed regularly, and that all updates are shared with relevant individuals at the earliest opportunity.
4. Monitoring procedures are open and transparent.

5. Allegations of misuse or known incidents are dealt with appropriately and promptly, in line with agreed procedures, and in liaison with other agencies where applicable.
6. Effective online safeguarding support systems are put in place, for example, filtering controls, secure networks and virus protection.

The Designated Safeguarding Officer (DSO) will be responsible for ensuring:

a) Agreed policies and procedures are implemented in practice
b) The importance of online safety in relation to safeguarding is understood by all ICT users through the pastoral programme.
c) The training, learning and development requirements of staff members are monitored and additional training needs identified and provided for.
d) An appropriate level of authorisation is given to ICT users. Not all levels of authorisation will be the same – this will depend on the position, work role and experience of the individual concerned. In some instances, explicit individual authorisation must be obtained for specific activities where deemed appropriate.
e) Any concerns and incidents are reported in a timely manner in line with agreed procedures
f) The college's pastoral programme addresses online safety
g) A safe ICT learning environment is promoted and maintained.

All staff members will ensure:

- The timely reporting of concerns in relation to alleged misuse or known incidents, subject to agreed procedures.
- ICT equipment is checked before use and all relevant security systems judged to be operational.
- Awareness is raised of any new or potential issues, and any risks which could be encountered as a result.
- Learners are supported and protected in their use of online technologies – enabling them to use safe ICT in a safe and responsible manner.
- Learners know how to recognise and report a concern.
- All relevant policies and procedures are adhered to all times and training undertaken as required.
- Learners are encouraged to:

    i. Be active, independent and responsible learners, who contribute as appropriate to policy and review.
    ii. Abide by the Acceptable Use Agreement.
    iii. Report any concerns through the IT manager or Safeguarding Team.

9 Contracts

Students should be aware that enforceable contracts may be formed over the internet and e-mail, and students should therefore take care to avoid entering into any written commitments which might be legally binding where they do not have the appropriate authority to do so.

10 Other forms of IT systems

The College uses surveillance equipment, in accordance with the Data Protection Act, in order to ensure the safety of its staff and students and security of its property. The College recognises the right of individuals to privacy and hence use of this equipment is restricted and would only be used for other purposes after appropriate staff had been advised of the intention to do so.

11 Charges

All charges due (e.g. for manuals, printouts etc.) must be paid at the time of receipt of goods. No credit is permitted.

12 Penalties

Anyone found to have broken these rules or otherwise misused IT facilities may have their computer account locked. If locked out of the system, you should report to the IT Support team in the LRC during normal opening hours. An appointment will be made as soon as is possible with a representative of IT Support.

There are a range of penalties which may be imposed depending on the nature and severity of the misuse, and whether it is a first or repeat offence. In each case IT Support will consult with the relevant member of staff which could include a Senior Manager in order to make a decision about the appropriate course of action. Penalties include:

- a warning about the action that might be taken in the event of further incidents of misuse
- a period during which access to IT systems and facilities is removed or limited
- obtaining a written agreement that the offence will not be repeated
- at any time it may be necessary to inform HR, Senior Leadership or external bodies of any breach of College rules regarding IT facilities

Other sanctions may be applied where justified by the offence. An offender may be required to pay all costs of any damage to any equipment supplied by the College, and related costs including staff time, hire of equipment etc.

Where offences are serious or persistent, the matter will be referred to the Senior Leadership Team to be considered under the College's Disciplinary Rules and Procedures.

13 Theft and vandalism

Any case of deliberate theft or vandalism may result in referral to the Senior Leadership Team for consideration under the Disciplinary Rules and Procedures and/or in prosecution.

14 Devices

Devices are brought into the college entirely at the risk of the owner and the decision to bring the device in to the college lies with the user as does the liability for any loss or damage resulting from the use of the device in college.

The college accepts no responsibility or liability in respect of lost, stolen or damaged devices while at college or on activities organised or undertaken by the college.

The college accepts no responsibility for any malfunction of a device due to changes made to the device while on the college network.

The college recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the college. Pass-codes or PINs should be set on personal devices to aid security.

The college is not responsible for the day to day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.

Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements

Users are responsible for keeping their device up to date through software, security and app updates

Users devices are only to be connected to the Eduroam and Guest wifi networks provided. They should not be connected the physical network without the express consent of the IT Manager.

15 The College reserves the right to change this policy from time to time as may be deemed necessary.

Passwords

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of St David's Catholic College's entire curriculum or admin network. As such, all St David's Catholic College students/employees (including contractors and vendors with access to St David's Catholic College systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all staff / students who are responsible for an account on the network at St David's Catholic College.

Policy

- All user passwords must be changed every term.
- User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.

Guidelines

General Password Construction Guidelines

Passwords are used for various purposes at St David's Catholic College. Some of the more common uses include:
User level accounts, email accounts, screen saver protection and voicemail password.

Poor, weak passwords have the following characteristics:

- The password contains less than six characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:

    - Names of family, pets, friends, co-workers, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./).
- Are at least eight alphanumeric characters long.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line.

Password Protection Standards

Do not use the same password for St David's Catholic College accounts as for other non-St David’s Catholic College access (e.g., personal e-Mail account, social media etc.). Where possible, do not use the same password for various St David’s Catholic College access needs. For example, select one password for the MIS systems and a separate password for IT systems. Also, select a separate password to be used for a ‘normal’ account and a UNIX account.

Do not share St David’s Catholic College passwords with anyone, including administrative assistants or secretaries.

All passwords are to be treated as sensitive and confidential St David’s Catholic College information.

Here is a list of "Don’ts":

- Do not reveal a password over the phone to ANYONE
- Do not reveal a password in an email message
- Do not talk about a password in front of others
- Do not hint at the format of a password (e.g., "my family name")
- Do not reveal a password on questionnaires or security forms
- Do not share a password with family members

If someone demands a password, refer them to this document or have them contact IT Support.

Do not use the "Remember Password" feature of applications (e.g., Outlook Express, Internet Explorer).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including mobile phones or similar devices) without encryption.

Password changes are automated every 90 days for most systems. If a system does not request a change automatically then it is good practice to change it at least once a term.

If it is suspected that an account has been compromised, report the incident to IT Support and change all passwords.