| Policy | Information Technology Policy - HR 15 |
|---|---|
| **Document owner** | Head of Digital Services and Technology |
| **Date first implemented** | June 2001 |
| **Date last reviewed** | May 2023 |
| **Date of next review** | May 2024 |
| **Date governor-approved** | |
| **Associated documents** | Data Protection Policy<br>Retention Schedule Policy |
| **Reference documents** | *UK Council for Child Internet Safety – Byron Review December 2009* |
| **Initial reviewing body** | Technology department |
| **Final approval body** | Senior Leadership Team |
| **Published on website** | No |

| | |
|---|---|
| **Purpose** | The IT policy outlines the College's approach to the use of information technologies throughout the organisation. The policy is designed to create a positive, creative and safe culture within the organisation towards the use of technology as a tool for inclusive learning while safeguarding the College, stakeholders and systems. |
| **Scope** | All staff and students, and users of the College's IT systems.<br><br>The principles of this policy apply equally during working hours and in personal time while ~~on-site~~on-site as well as offsite on all equipment connected to the network. |
| **Equality, Diversity & Inclusivity** | *"[Derwen] College is committed to promoting equality, good relations and to challenging discrimination. This is reflected in all College policies, procedures, processes and practices."*<br>*Derwen College Equal Opportunities Policy*<br><br>Derwen College's ethos is to embrace diversity, to offer equality of opportunity, and to treat every individual fairly and with respect. Equality, diversity and inclusivity are embedded throughout the organisation. This policy should be applied in accordance with this ethos.<br><br>If you would like a copy of this document in a different format, such as large print, please contact the Human Resources Department who will provide help with alternative formats. |

Derwen College aims to offer access to appropriate resources and training to be innovative in the application and knowledge of new, emerging and SEND assistive technologies to enhance the learner experience in all areas of the curriculum.

While the college recognises and accepts users will use the college systems and

internet facilities for personal use, it does expect certain standards of conduct to be observed to protect both the college interests and its employees from the dangers of inappropriate use.

All information residing on the College systems is the property of the College.

In order to fulfil its policy the College will:

- include systems to ensure content is safe and neither derogatory or inappropriate
- provide development opportunities to staff appropriate to the changing developmental and technology needs within the context of their role in the College
- ensure that opportunities are provided to expand staff and students' knowledge of information technologies and their application
- provide appropriate support and assistance
- provide learning resources appropriate to support a range of IT needs
- monitor and support the integration of IT across all areas of the College
- ensure that information technologies are used appropriately to enhance and support the learning environment in creative and innovative ways
- use recognised industry standard platforms appropriate to the user environment to ensure that the uses of information technologies are not restricted by inappropriate compatibility limitations
- make sure students' prior ~~technological~~ technical skills and knowledge are identified to support access to their individualised learning programmes
- make training available to all students that will enable them to progressively develop their IT skills
- provide access to new and emerging technologies as a tool for continued development and electronic or augmented communication
- continue to research, develop and exploit future developments in information technologies
- continue to research, develop and exploit future developments in SEND assistive technologies
- maximise the use of College resources through cross curriculum collaboration
- provide an appropriate upgrade and replacement strategy for hardware and software resources
- develop and maintain a dynamic website
- ensure that staff change their passwords on a regular basis in line with password policies
- enhance cyber security
- maintain appropriate and proportional multi-layered backups
- review and assign administrative rights to staff based on job requirements
- comply with copyright and data protection legislation
- use the self-assessment process to evaluate the effectiveness of the technology provision
- monitor its IT systems as is deemed necessary in order to prevent inappropriate usage
- provide staff with cyber security CPD

## 1. Network

The College will:

- reserve the right to review and monitor all content on the College systems (i.e. folders, emails, internet use, real-time usage)
- keep backups of all data in line with the backup procedure, Data Protection Policy and Retention Schedule Policy
- reserve the right to restore backup information
- reserve the right to remove access to the network
- keep the network up to date to meet the cyber security needs of authority partners

All users must:

- take care not to introduce malicious content ~~on to~~onto the system
- not send or forward inappropriate content
- take responsibility for the safety of the College network and its users
- keep passwords private
- not use someone else's log-on details or leave your system open to allow access to others
- report any potential breach of network security straight away to the IT helpdesk
- not delete, copy or remove off site any content from the College systems prior to leaving employment
- not attempt to circumnavigate security and compliance systems (e.g. web filter, firewall)
- seek approval ~~by~~ from the Technology department before purchasing any equipment to be used on the network (not including BYOD)

Staff must:

- not allow students access to equipment specifically configured as a staff device or that is joined to the staff network
- not allow students access to their account
- abide by the password policy (section 2)

## 2. Passwords

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorised access and/or exploitation of Derwen College resources. All users, including contractors and vendors with access to Derwen college systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords (Student passwords are not subject to this for ease of use).

A. Passwords for all systems should consist of 8 or more characters, consisting capital letters, lower case, numbers and at least 1 special character (@#!).
B. Where possible, users must use unique or a varied password between systems unless the system in question has synchronised single sign on.
C. User accounts that have high system-level privileges or administrator accounts must have a password that is unique, and different from all other accounts.
D. Passwords must not be revealed over the phone to anyone.
E. Do not write down passwords and store them anywhere that isn't secure.
F. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords immediately.
G. Passwords must not be shared with anyone. All passwords are to be treated as sensitive.
H. Passwords must not be inserted into email messages or other messaging services.

I. Do not share passwords with anyone at any time
J. Do not leave any pc, laptop or device unlocked while unattended. Any unattended device must be locked or logged off~~.~~
K. Users with access to privileged or sensitive information must use multi-factor authentication (2FA or MFA) when accessing resources externally
~~K.~~L. Where possible, use Windows Hello to enhance security via password-less multi-factor authentication

## 3. Internet and email (including use with BYOD (Bring Your Own Device) and externally)

The College will:

- provide a web filtering service and internal firewall controls to ensure safety of systems and content (blocked sites to be reported to the technology staff)
- not impose time limits on internet use for staff providing it does not interfere with working practices
- limit Wi-Fi access for students at night
- provide an email platform
- reserve the right to monitor emails, cloud documents and social media activity
- monitor in real-time, via Smoothwall, all sites accessed by staff, students and visitors

All users must:

- use the internet and emails sensibly and in such a manner that it does not interfere with the efficient running of the College or go against the College's safeguarding policies
- not access illicit websites and websites outlined below (not exhaustive, more details of blocked sites can be provided by the ICT helpdesk or safeguarding team):
    - Pornography
    - Adult sites
    - Child abuse
    - Dating and companionship ~~(within college hours)~~
    - Drugs
    - Gambling
    - Hacking
    - Terrorism
    - Violence

*Note: All websites views are stored, can be seen in real-time and reported on. Any breaches will be recorded and be passed on to the safeguarding team (students/clients) and HR (staff). If appropriate, external agencies and/or law enforcement may be involved*

- treat emails as formal communication that they will be accountable for
- get approval from the Technology department before signing up ~~to~~ for online subscription services or licensing contracts
- exercise great caution before opening emails with attachments from unidentified third parties to reduce the risk of viruses (if in doubt seek assistance from the ICT helpdesk)

- use the College-provided email address and platform to communicate ~~to~~ with students via email
- not use file sharing applications or download copyright material

Staff must:

- not engage in any personal online contact or share personal details with current or former students without prior approval from the relevant line manager (if in doubt contact ~~the E-Safety Coordinator~~the safeguarding team)
- not use Whatsapp or social media (or similar non-college platforms) to contact students
- ensure that personal details/photos/videos/social media etc. are not accessible to students or ex-students as this is outside acceptable professional boundaries

## 4. BYOD (Bring Your Own Device)

All private hardware and software ~~is~~ are used at the owner's discretion and the College takes no responsibility for damage or breakages. The equipment will also not be covered by the college's insurance.

The hardware and software must also comply ~~to~~ with copyright laws.

The College will:

- provide secure Wi-Fi access for staff, students and visitors
- allow staff and students to bring their own devices into College
- reserve the right to remove or not allow access
- log all internet usage from the device

All users must:

- use their own unique college-provided user account to access the internet
- connect to the correct and appropriate WIFI SSID
- not use 3G/4G/5G or other mobile internet services to circumnavigate network restrictions
- where appropriate and the device allows, have anti-virus protection
- be up to date with the latest software version
- exercise caution and vigilance to ensure content is secure when using portable devices (i.e. memory sticks/laptops/tablets) to use any College information, confidential or not
- take great care when bringing in personal content on their own devices that such content is appropriate
- ensure all inappropriate tabs or apps are closed
- not link their device to the wired network unless permission has been granted by the Technology department

Staff must:

- not use personal devices to record, photograph and film students
- not allow students access to devices
- ensure that personal details/photos/videos etc. are not accessible to students or ex- students as this is outside acceptable professional boundaries

## 5. External access

The College will:

- Provide external access via a secure always-on VPN to the network via a ~~college provided~~college-provided router, laptop or PC to staff that have been permitted to work from home
- Provide external access to emails (webmail) and O365 applications to all users
- Reserve the right to remove remote access at any time

Staff must:

- Use the equipment as if they were within the College campus
- Abide by all College ~~polices~~ policies regarding information technology, data protection and safeguarding
- When accessing external services such as emails, Sharepoint or college cloud services, to use the services as if they were in college and abide by the college's policies
- Report any concerns, breaches or failures to the ICT helpdesk immediately
- Not allow third parties to use the equipment
- ~~Where applicable, a~~abide by the staff laptop agreement

## 6. Software and databases

The College will:

- Provide software, data platforms and databases to facilitate the running of the College, curriculum and commercial activities
- Keep all platforms up to date
- Where possible, enforce data protection, GDPR, data retention and safeguarding policies
- Reserve the right to remove access

All users must:

- Seek permission from the Technology department before purchasing or implementing new software platforms, databases or software packages
- Ask the ICT helpdesk to install new software platforms, databases or software packages
- Abide by data protection, GDPR, data retention and safeguarding policies
- Not allow unauthorised access to platforms
- Not share access to platforms
- Not copy, report or redistribute software platforms, databases, software packages or data contained within any of the platforms without permission from the technology department
- Not provide details of software platforms, databases or software packages to third parties without prior permission of the technology department
- Where possible, use the ~~colleges~~ college's main management information system and linked software as the basis of information concerning students and curriculum

## 7. Technology standard operating procedures (SOPs)

The College will:

- Where appropriate create SOPs for key data and procedural tasks

All users must:

- Follow SOPs when provided
- Report any failures or areas for improvement within the SOP to their line manager
- Treat the SOP as confidential unless made available

## 8. Disposal of waste

The Network Manager should ensure that any personal or sensitive data is erased from College technology equipment on its disposal or transfer from the College. The need for disposal extends to software stored on the equipment for which the College holds the licence. Also, any information that can provide access to the network or provide insights to the network such as IP structures.

When disposing of the equipment the Network Manager must ensure that the requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed.

## Disciplinary action

Breaches of this policy will be subject to disciplinary action in accordance with the College's disciplinary procedure.

Any comments made on either email or social media sites inside or outside the workplace that are defamatory, derogatory, or discriminatory about the College, colleagues and its stakeholders will not be tolerated and investigated as gross misconduct. If substantiated, such conduct may lead to summary dismissal after the due process of the College's disciplinary procedure has been followed.

The College will monitor its IT systems as is deemed necessary in order to prevent inappropriate usage. Hard copies of blog entries will be used in any disciplinary proceedings. Social media entries may create documents which the courts can order to be disclosed for use in litigation. Consequently, employees will be assumed to have written any contentious items unless they can prove definitively that they have not done so.