Cardiff and Vale College
Coleg Caerdydd a'r Fro

***There is a Welsh version of this document available.***

# IT Security Policy

## Scope and Purpose of Policy

The purpose of this policy is to define a framework on how to best protect the college's computer systems, network and all data contained within, or accessible on or via these computer systems from threats whether internal, external, deliberate or accidental.

IT Systems play a major part in the operation of the College. The availability, confidentiality and the integrity of data on the College IT Systems is critical to the success of our academic and administrative activities. Effective security is achieved with discipline, in compliance with legislation and adherence to College procedures.

It is the Policy of the College to ensure that:

- All central computer systems, programs, data and network will be adequately protected against loss, abuse or unauthorised access.
- All members of the College are aware that is it their responsibility to adhere to this policy.
- All regulatory and legislative requirements regarding computer security and information confidentiality and integrity will be met by IT Services and the College.
- Create across the college awareness that appropriate measures must be implemented as part of an effective operation of IT Security.
- Ensure all users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle.

This policy is underpinned by the Group's vision – Inspirational, Inclusive and Influential - and will support our work towards the strategic priorities of Quality, Efficiency, Growth and Wellbeing. The policy will incorporate the following principles:

- Learners will be supported to enable them to achieve their potential whilst in learning, in an environment which removes or minimises disadvantage, takes steps to meet their needs and which encourages participation.
- The College will support learners to develop the skills they need to progress successfully through their lives.
- A commitment to the social model of disability where we look at removing the barriers someone could face because of their disability or learning difficulty to promote inclusion.

The Policy applies to all staff and students of the College.



| | |
|---|---|
| **Revision No:** | 4 |
| **Last Revision Date:** | Oct 24 |
| **Next Revision Date:** | Oct 26 |

## Overarching Responsibilities

The IT Security Policy sets out the responsibilities for ensuring the security of IT Systems, the procedures to be followed and the confidentiality and integrity of the information held.

- The integrity of all central computer systems, the confidentiality of any information contained within or accessible on or via these systems is the responsibility of IT Services.
- The College Executive Management Team is responsible for approving the IT Security Policy and for ensuring it is implemented in academic and support departments.
- All college staff are responsible for the immediate reporting of any security-related incident to their line manager. The IT Operations Manager is responsible for co-ordinating investigations into any reported IT security incidents.
- The IT Operations Manager shall take the appropriate steps to ensure that staff are informed of their obligations under the Data Protection Act, The Acceptable Computer Usage Policy and Software Copyright Legislation.
- The College's internal auditors, overseen by the Audit Committee, will periodically review the adequacy of IT systems controls as well as compliance with such controls.

## The ICT environment

IT Services plan, maintain and operate an extensive range of servers, network devices (core, edge and wireless), storage systems, backups and interconnectivity of all these systems and college campuses.

The computer environment is defined as all computer resources and network infrastructure managed and overseen by IT Services and all computer devices that physically connect, and have been authorised to connect, to this environment. All are covered by this policy, including hardware and software, College-related data residing on these machines or accessible from these machines within the campuses network environment, and any portable media that may at times be accessible.

IT Services consider all temporary and permanent connections via the College network (via any type of client device, wireless or wired, or via remote access) to be subject to the provisions of this policy.

Computer assets not owned by the College (e.g. devices owned by students or visitors) are only permitted to connect to the College via wireless network. Under no circumstances are non-college assets to be connected to the College network via a wired connection.

IT Services reserve the right to monitor, log, collate and analyse the content of all transmissions on networks maintained by the College if deemed necessary for performance, fault diagnostics, suspect security breaches or investigation purposes.

## Physical Security

IT Services have a secure communications room with the following criteria:

- Secure Lockable doors and locked cabinets.
- Dedicated clean power supply with separate distribution board and isolation controls.
- Duty and standby air conditioning control units in main server locations.
- Power distribution.
- Passive cable management in most cabinets.

Any computer equipment in offices or classrooms should be in a room which has locked doors and is always staffed when open.

## Access to College IT Systems

- Computer and network systems access is only via individual user accounts. The use of generic accounts is only permitted for certain activities where personal accounts are unavailable, e.g. initial assessment testing prior to accounts being created. All staff will have accounts created upon commencement of employment. All students have accounts created once enrolled onto the College MIS system. This ensures that all accounts can be audited and users are accountable.
- All users have access to shared file resources. Use of this data is covered in the Computer Acceptable Usage Policy.
- All data will be controlled by Security groups. Any request for access to information must be requested through IT Services.
- The use of email is governed by the Computer Acceptable Usage Policy. The College subscribes to an external spam and virus filtering service to ensure, as far as possible, the integrity of mail being delivered.
- All users have access to the internet. Control measures are in place to monitor and report on usage.
- Users should not in any way use personal web space or social networking sites to publish such material which deliberately undermines IT Security at the College or defames the College's name or any individuals in the College.
- All users must adhere to the College's Social Media Policy.
- All College systems sit behind firewalls.
- The College network is connected to the Joint Academic Network (JANET) - a high-speed network for the UK research and education community provided by Jisc, a not-for-profit company set up to provide computing support for education. The College must comply with Janet Regulations.
- IT Services will disconnect any machine from the College network which hasn't been installed by the IT Services Department.

- Remote access to some college services is available for both students and staff, e.g. Moodle, intranet. For a remote connection to be established, a valid domain account on the college network is required for authentication to any College IT resources. The college has a facility for staff only to access further network resources via VPN or remote Wi-Fi access point. This applies to College-owned equipment only and should be requested via IT Services. Limitations on the number of connections permitted are in place.
- IT Services do not support home users' machines.
- Anti-Virus software is deployed on all clients and is kept is up-to-date. If a user suspects an infection, a complete scan may be performed at the discretion of IT Services.

## Review of Security

Periodic risk assessments will be undertaken to assess the IT Security controls in place, in order to take account of changing business requirements and any changes in legislation.

## Breaches of Security

IT Services will monitor network activity, reports from other security advisors (e.g. Antivirus, Microsoft), and take action/make recommendations consistent with maintaining the security of the College IT Systems.

Any user suspecting that there has been, or is likely to be, a breach of IT Security should inform their line manager who should inform the IT Operations Manager to determine what action should be taken.

In the event of a suspected or actual breach of security, the IT Operations Manager may, in consultation with HR or the Executive Management Team, make inaccessible or remove any unsafe user, account, service or connection to IT resources in order to safeguard the College IT Systems.

Any breach of IT security could result in loss of personal information. This would be an infringement of the Data Protection Act 1998 and could lead to civil or criminal proceedings. It is therefore vital that users of the College IT systems not only comply with this policy, but also with the College's Data Protection Policy.

The IT Operations Manager has the authority to take whatever action is deemed necessary to protect the College against security breaches.

## Status of the IT Security Policy

This policy does not form part of any formal contract of employment with the College, but it is a condition of employment that employees abide by the regulations and policies made by the College from time to time.

## Responsibilities

The Governing Body is responsible for ensuring that:

- The Policy is reviewed on a regular basis (as per the policy terms of review) and appropriate advice is given on content. The Main Board approves the policy.

The Executive and Senior Leadership Team are responsible for:

- Ensuring that the College's IT Security Policy and procedures are fully implemented and followed by staff.
- Reviewing this Policy and the attached procedures.
- Monitoring the application of the procedures, supporting staff to adhere to the policy and responding effectively to any areas of concern.
- Ensuring that relevant college procedures and practices, e.g. admissions, tutorials etc. embed IT security procedures.
- Ensuring sufficient resource is allocated to this area.
- Ensuring the allocation of appropriate resources to meet the requirements of the policy and associated procedures.
- Maintaining the currency of this policy and associated procedures.
- Providing appropriate training and development.
- Ensuring that appropriate steps are taken to monitor data linked to this policy and that this data is used to inform and improve practice.

All staff are responsible for:

- Treating all learners with dignity and respect, to ensure their own conduct does not cause offence or misunderstanding.
- Being aware of this policy and the procedures and working in a way that does not contravene their contents.
- Working within the requirements of Data Protection and GDPR.
- Communicating effectively with staff to ensure the needs of learners are met.
- Attending CPD events on aspects relevant to the success of this policy and associated procedures.

Students are responsible for:

- Attending induction and tutorial sessions to ensure they are aware of the policy and the issues it raises.
- Behaving in a way that supports the Policy across college.

- Contributing to learner surveys and focus groups to provide feedback on this policy and associated procedures and how it impacts on them.

## Legislation and Guidance

The College has an obligation to abide by all UK legislation and relevant legislation of the European Community. Of particular relevance are the following:

- Regulation of Investigatory Powers Act 2000 (RIPA)
-

- Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000.
- The Data Protection Act 2018.
- The General Data Protection Regulation (GDPR) 2016.
- The Human Rights Act 1998
- The Copyright, Designs and Patents Act 1988.
- The Computer Misuse Act 1990.
- Freedom of Information Act 2000.

## Equality and Diversity Statement

In accordance with College procedures, this Policy was written with consideration of the impact of individuals as per the Equality Act.

## Health and Safety Implications

None.

## Welsh Language Standards

This policy provides opportunities for persons to use either the Welsh or English language. The duties which come from the Standards mean that organisations should not treat the Welsh language less favourably than the English language, together with promoting and facilitating the use of the Welsh language i.e. making it easier for people to use in their day-to-day life.

## References

## Linked Policies

- Freedom of Information
- Equality and Diversity
- Disclosure
- Safeguarding

- Complaints, Comments and Compliments
- Social Media
- HR – Disciplinary
- HR - Grievance

## Linked Procedures

- Data Retention
- Freedom of Information
- Equality and Diversity
- Disclosure

- Safeguarding
- Dress Code
- CAVC Privacy Notice
- Staff Privacy Notice
- Complaints, Comments and Compliments

## Communication and Storage

This policy is published on the company website.
This policy is stored on the company intranet.
This policy is shared with learners.

## Glossary

None

## Approval, Change and Review

This policy is reviewed every two years.

There is a Welsh version of this document available.

| | |
|---|---|
| **Date approved:** October 2024 | **Responsible Manager:** IT Operations Manager |
| **Approved by:** Main Board | **Executive Lead:** Group Chief Operating Officer |
| **Next Review date:** October 2026 | **Accessible to Students:** Yes |