θ

Reference:	CGISMS-POLICY-ISF01-PUBLIC
Version:	1.1
Date approved:	July 2024
Approved by:	Corporation Board
Name and title of policy holder:	Diane Clark, Director of ICT
Review date:	July 2025

Version	**Type – New/Replacement/Review**	**Date**

Page

INFORMATION SECURITY FRAMEWORK

INTRODUCTION

Good practice with regards to the use of Information Technology (IT) security is an essential element in providing the technical applications and infrastructure that underpin and support the teaching, learning, and administrative activities of the College.

The College must: -

Each incident should be investigated and reported within 7 days of occurrence or notification of the incident. If criminal action is suspected, the College may consider contacting the police immediately. Any security breach by a staff member or learner will be subject to the college's Disciplinary policy, Anti- Fraud Policy, or the Learners Code of Conduct.

It is the responsibility of all staff and learners to report all concerns and incidents as follows:

MONITORING

Policy	Reporting Manager	Name	How to report
Acceptable Use	Director of ICT	Diane Clark	Email: diane.clark@coleggwent.ac.uk
E-Safety	Safeguarding Officers	BGLZ: Laura May Aylett Crosskeys: R Td [(I)-5.5 (CT)]TJ 0 Tc 0 Tw 1.261 0 Td ( )Tj EMC E	

No member of staff is permitted, as a matter of routine, to monitor or investigate an individual's use of Coleg Gwent ICT resources. However, where there are reasonable grounds to suspect an instance of

POLICY STATEMENT

The College seeks to promote and facilitate the positive and extensive use of Information Communication Technology in the interests of supporting the delivery of learning, teaching, and operational/administrative activities.

PURPOSE AND SCOPE

The Acceptable Use Policy defines what is deemed:

1. acceptable use of Coleg Gwent ICT resources;
2. unacceptable use of Coleg Gwent ICT resources;
3. acceptable practices in preserving the confidentiality, integrity, and availability of Coleg Gwent information.

The policy applies to all users (refer to page 1 for definition of users) and should be read in conjunction with other relevant college policies e.g. Data Protection, E-Safety, Information Security, and learner / staff disciplinary policies.

POLICY

1. **ACCEPTABLE USE – ICT RESOURCES**

- Users are issued with a username and password which must be used to authenticate and gain access to ICT resources. The password must be kept confidential and must not be shared with anyone else. Passwords must be changed immediately if a user suspects it has been compromised. Suspected compromise of passwords must be reported to the ICT department.

- Users are responsible for all activity that takes place under their username and must not allow anyone else to access ICT resources using their username and password. This extends to usernames and passwords issued by third parties where college data is stored e.g., Awarding Body websites. Where access to third party sites is hindered due to long term staff sickness absence, the manager of the department must seek advice from the ICT department.

- Users must never ask for passwords or login details of any other CT.5 (nc)-8 (e)9.3 (s1-4.6 wC-1.5 (y2w 2.065

studies. Excessive personal use during college hours could be considered a disciplinary offence.

- Any suspicious activity such as viruses, phishing emails, malware, or ransomware must be reported to the IT department during college hours.

- Attempting to install software or hardware without first seeking advice and permission from the ICT department.

- Storing information on internal storage areas that are not routinely backed-up e.g. computer hard-drive. However, if technical issues prevent users from accessing shared drives or cloud repositories, it is permissible to use the internal storage area on I1.5 (r)-74 0 Td( )Tj-0.813 Tc 0.003 Tv

POLICY STATEMENT

This policy reflects the need to raise awareness of issues associated with the safe use of technology.

PURPOSE AND SCOPE

The E-Safety Policy is designed to raise awareness with learners and staff in relation to working safely with technology and in doing so, support users to understand associated risks & their own personal responsibilities. The policy should be read in conjunction with other relevant college policies
e.g. Acceptable Use Policy, Safeguarding, Protection of Children & Vulnerable Adults, Anti Bullying, Communication, Data Protection, Learner and Staff Disciplinary Policies & Procedures.

POLICY

1. CONDUCT

The line between public and private, professional, and personal is not always clearly defined when using technology. When engaging in either in a professional or personal capacity, staff and learners must act appropriately. Examples of appropriate behaviour that all users must follow include:

- being professional, courteous, and respectful;
- being transparent and honest;
- thinking carefully about how and what activities are carried out; and
- removing or requesting the removal of any inappropriate comments or images.

Users must be aware of the consequences of acting inappropriately, examples of inappropriate behaviour include:

- making comments that could be considered to be bullying, harassing or discriminatory against any individual;
- using offensive, derogatory, or intimidating language and writing styles;
- knowingly accessing, viewing, or downloading material which could cause offence to other people or may be illegal;
- uploading inappropriate comments, images, photographs and/or videos;
- publishing defamatory and/or knowingly false material;
- participating in any activity which may compromise your position at the College;
- engaging in activities that have the potential to bring the College into disrepute;
- breach of confidentiality by disclosing privileged, sensitive and/or confidential information; and
- posting any material that breaches copyright legislation.

2. SOCIAL NETWORKS

The College recognises the value that social media can have to our business and personal lives if used in a responsible and professional way. Whilst it is recognised that staff and learners are entitled to a private life; the College is committed to maintaining confidentiality and professionalism at all times. Staff who utilise social networks must exhibit acceptable behaviours.

12. PREVENT MMPREVENT

Where an E-Safety incident is reported to the college this matter will be dealt with very seriously. The college will act immediately to prevent as far as reasonably possible any harm or further harm occurring. Following any incident, the college will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place; external agencies may be involved and the matter will be dealt with in accordance with the disciplinary policy. This is in line with the college Acceptable Use Policy. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

POLICY STATEMENT

Information is critical to College operations and failure to protect information increases the risk of financial and reputational losses. The College is committed to protecting information, in all its forms, from loss of confidentiality, integrity and availability. The College will ensure that ICT resources and the information that it manages (both manual and electronic) is appropriately secured to: -

- ensure compliance with relevant legislation and guidance;
- protect against unauthorised access;
- ensure confidentiality is maintained, especially where third party or personal data is held;
- ensure business continuity and the protection of assets; and
- prevent failures of integrity, or interruptions to the availability of that information.

PURPOSE AND SCOPE

The Information Security Policy outlines the College's approach to information security management and provides the guiding principles to ensure the College's information security objectives are met. This policy should be read in conjunction with other relevant college policies e.g. Acceptable Use, Data Protection, E-Safety, Archive/Retention of Documents, Safeguarding, Protection of Children & Vulnerable Adults, Anti Bullying and Communication.

The policy is applicable across the College and individually applies to:

- all individuals who have access to Coleg Gwent information;
- all individuals who have access to Coleg Gwent ICT resources;
- all facilities, technologies and services that are used to process Coleg Gwent information;
- information processed, in any format, by the College pursuant to its operational activities;
- internal and external processes used to process College information; and
- external parties that provide information processing services to the College.

POLICY

1. **INFORMATION ASSET MANAGEMENT**

   Information asset owners are identified for all College information assets, assets are classified according to how critical and sensitive they are, and rules for their use are in place. Coleg Gwent ICT resources must be effectively managed and kept secure from theft and damage. Redundant Coleg Gwent ICT resources will be disposed of securely, and in doing so all data will be removed.

2. **INFORMATION SECURITY CONTROLS**

   Appropriate information security controls are implemented and monitored to protect all Coleg Gwent information assets.

3. **ACCESS CONTROLS**

   Only individuals with approved access to information assets can actually access them, and this is subject to both logical and/or physical barriers. Sufficient access levels will be provided for individuals to undertake their role. Where logical access controls are in place e.g. passwords, these will be subject to mandatory resetting at set intervals.

Coleg Gwent information assets must be protected from unauthorised access, accidental or malicious damage, loss, and theft. Only approved Coleg Gwent ICT resources will be installed on the network and unauthorised resources will be removed.

4. DATEp1

POLICY STATEMENT

The College collects and processes large amounts of personal data in order to perform its tasks and obligations. It is committed to protecting this data from point of collection through to point of destruction by ensuring robust procedures and security measures are implemented within the college.

5 0 Td( )Tw

3. **LAWFUL, FAIR AND TRANSPARENT PROCESSING**

The College will maintain an asset register of all systems used to process personal data in the College. Asset Owners will be assigned for each department. The register will be reviewed annually.

Individuals have various rights to their personal data under UK GDPR/DPA 2018. They will be informed of these rights via the college's privacy notices held on the website and via fair processing notices on application/enrolment forms.

Requests like this will be dealt with promptly by the Data Protection Officer (DPO). Relevant procedures for these requests will be implemented and maintained by the DPO.

The college uses CCTV for the prevention and detection of crime and for educational purposes. Systems are positioned to view college sites and boundaries only. Data is retained in line with the college's retention schedule.

4. **DATA MINIMISATION AND ACCURACY**

Personal data collection will be adequate, relevant, and limited to only what is necessary to meet the legal basis for processing. Steps will be taken to ensure personal data remains accurate via appropriate college procedures.

5. **ARCHIVING AND DISPOSAL**

Personal data will be retained for no longer than necessary for the purpose for which it was collected.

Archived information held with the college's approved storage company, will be subject to the same security as data held within the college. A record of retention periods will be available in the college's retention schedule and financial control procedures. Details of Welsh Government retention durations will be stated within the college's external privacy notices.

Personal data, including personal data contained within informal records, will be destroyed by secure methods such as shredding or via the college's approved contractors. Staff must ensure confidential waste is kept in a secure, locked location prior to collection for disposal. Electronic records will be destroyed by secure means, following the college's ICT procedures.

Specific responsibilities are outlined in the Coleg Gwent0,0 Tc 0 Tw ( )304 Tw 7 0c.435 -1.163 Tda72 0 Td

Staff will undergo annual data protection and cyber security training.

Personal data will be kept IS0.03.6 (l)-1.5 (l)-1.74J0 Tc 0 Tw 3.Tc 0 Tw (11.3 ak)1 (d[s5w (w (11.3 Tc 0 T

DATA PROTECTION POLICY

10. RESPONSIBILITIES

Tc -0.012 Tw 8.466 -0 0 9.9 re.48 754.44 Tm[(r)15.7 (es)

Governing Body Ultimately yes

DATA PROTECTION POLICY