Coleg Gwent

INFORMATION SECURITY FRAMEWORK

Equality Impact Assessment:	**17/10/2022**
Welsh language Impact Assessment:	**17/10/2022**
Approved by:	**Board**
Author:	**Director of ICT, Diane Clark**
Date Approved:	**13/12/2022**
Review Date:	**12/2023**

Reference:	CGISMS-POLICY-ISF01-PUBLIC
Version:	1.0
Date approved:	December 2022
Approved by:	Corporation Board
Name and title of policy holder:	Diane Clark, Director of ICT
Review date:	December 2023

Version	Type - New/Replacement/Review	Date	History
1.0	New	Dec 2023	New document template Data Protection Policy incorporated into Framework Updated to align with Cyber E

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: -

i. ensure that its learners and staff remain safe in their use of technology; and
ii. protect its information assets.

In doing this, the college will: -

x

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: Ryan Chard Newport: June Bridgeman TLZ & Usk: Sian Hughes	Email: lauramay.aylett@coleggwent.ac.uk ryan.chard@coleggwent.ac.uk june.bridgman@coleggwent.ac.uk sian.hughes@coleggwent.ac.uk online via the staff & learner portals
Information Security	Data Protection Officer Director of ICT	Anna Lebar-Hill Diane Clark	Email:dpo@coleggwent.ac.uk diane.clark@coleggwent.ac.uk online via the staff & learner portals
Data Protection	Data Protection Officer Director of ICT	Anna Lebar-Hill Diane Clark	Email: dpo@coleggwent.ac.uk diane.clark@coleggwent.ac.uk online via the staff & learner portals

All email, internet use, telephone calls and other ICT usage is logged, and may be subject to automated monitoring. Monitoring may be carried out in compliance with applicable obligations under the UK General Data Protection Regulations (UK GDPR) and Data Protection Act 2018 (DPA 2018) and where this is permitted under the Regulation of Investigatory Powers Act 2000 (and associated regulations) for the purpose of:

- preventing or detecting criminal activities;
- investigating or detecting unauthorised use of the College's ICT resources;
- ascertaining compliance with regulatory or self-regulatory practices or procedures and standards; and
- ensuring effective system operation.

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 unacceptable use of any ICT resources, or where a legitimate request is made by the police or other authority, permission may be granted by the Vice Principal for the monitoring or investigation of an individual's use of College ICT facilities. This may include the monitoring of email, use of the internet and login attempts to accounts. Staff being monitored in line with disciplinary action will be informed of this via the HR disciplinary procedure.

The College has an explicit duty under s26(1) of the Counter-Terrorism and Security Act 2015 to have due regard to the need to prevent people from being drawn into terrorism. This requires the College to monitor and report on the use of relevant ICT facilities e.g. attempts to access terrorism websites.

The college will utilise monitoring devices and intrusion detection software to monitor network security. Any devices operating within the College network that present a security threat will be removed from the network.

CCTV systems in the College are used for the prevention and detection of crime and for educational purposes.

CCTV systems must be positioned to avoid capturing images of persons not visiting College premises. The recorded images must be stored safely and will only be retained for the necessary duration (this will vary depending on the specific equipment/location). Recordings will only be made available to third parties such as law enforcement agencies and insurance companies whose sole purpose is the prevention and detection of crime. The release of recordings must be approved by the Information Governance Manager.

CONSEQUENCES OF NON- COMPLIANCE

Non-compliance with the

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 ICT department immediately.

- Any Coleg Gwent ICT resource in the possession of a user, must be returned to the ICT department upon request, or when the user leaves the college at the end of their studies or upon the termination of an employment contract.

- All Coleg Gwent data or intellectual property developed or gained during the period of employment remains the property of Coleg Gwent and must not be retained beyond termination or reused for any other purpose.

2. UNACCEPTABLE USE – ICT RESOURCES

- Coleg Gwent ICT resources must not be used for the download, creation, manipulation, transmission, or storage of:
  a. any offensive, obscene, or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
  b. unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others;
  c. unsolicited "nuisance" emails;
  d. material which is subsequently used to facilitate harassment, bullying and/or victimisation;
  e. material which promotes discrimination on the basis of race, gender, religion or belief, disability, age, or sexual orientation;
  f. material with the intent to defraud or which is likely to deceive a third party;
  g. material which advocates or promotes any unlawful act;
  h. material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party;
  i. material that brings the College into disrepute.

- Intentionally or recklessly introducing any form of spyware, DDoS attack, computer virus or other potentially malicious software designed to adversely affect the operation of any Coleg Gwent ICT resource.

- Attempting to bypass or override any ICT security control measures.

- Causing reckless or intentional damage to Coleg Gwent ICT resources.

- Seeking to gain unauthorised access to restricted areas of the college network.

- Using Coleg Gwent ICT resources for personal commercial activity.

- 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. If staff have difficulty accessing areas during lessons or meetings due, for exampl7 0 Td[(t)-9.3 (h p -1.326 Td[(c)-9.1 (om3 (r)16.>1 (e)23xA (on)]TJ0 Tc 0 Tw 5.12 0 TW3 0 TW3 0 TW

-

- Coleg Gwent ICT resources and Coleg Gwent information that are taken off-site must not be left unattended and due care and attention should be exercised at all times e.g., do not leave a laptop on display in a car or leave files / class lists overnight in cars.

- The use of personal devices (by staff) to carry out Coleg Gwent activity will only be approved once the device has been checked to ensure it meets basic standards such as, the device is password protected, up to date anti-virus software, up to date operating system and the operating system has not been ‘jail broken’ or ‘rooted’.

- Users are only allowed to use authorised systems for processing personal and confidential data.

- Accessing, or trying to access information where the user knows wed5D8a6 (ng)h4 (nt)1.1.7 (c

E-made public through

12. PREVENT

INFORMATION SECURITY POLICY

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: -

x ensure compliance with relevant legislation and guidance;

x protect against unauthorised access;

x ensure confidentiality is maintained, especially where third party or personal data or

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. **WORKING WITH THIRD PARTIES**

All relevant information security requirements of the College should be covered in agreements with any third-party partners or suppliers and compliance against these must be monitored. An up-to- date record of all third parties that access, store, or process college information must be maintained.

5. **RISK MANAGEMENT**

Information security risk assessments must be carried out by the Director of ICT on all the College's infrastructure, systems, and processes on a regular basis to identify key information risks and determine the controls required to keep those risks within acceptable limits.

6. **COMPLIANCE**

Information security controls must be monitored to ensure they are adequate and effective. This will be done in numerous ways including internal audits and Cyber Essentials Plus accreditation.

7. **EDUCATION AND TRAINING**

The college will provide Information Security awareness training that all users of college ICT resources must complete.

8. **REPORTING CONCERNS AND INCIDENTS**

All information security incidents must be reported immediately via the appropriate reporting channel (refer to page 2). All incidents are effectively managed and resolved, and learnt from to improve our information security controls.

DATA PROTECTION

POLICY DEFINITIONS

Personal Data	Information relating to an identified/identifiable living individual
Identifiable Individual	Someone that can be identified directly (name/image) or indirectly (ID number)
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data such as

Staff will undergo annual data protection and cyber security training.

Personal data will be kept securely on appropriate college systems within the network. Steps will be taken to ensure these systems remain up to date. Systems will be regularly tested to address any potential weaknesses.

No personal data processed and held by the college must leave the college's network unless authorisation has been sought to remove the data.

Where staff are approved to use a removable device to process personal data, the device must be pre-approved by the ICT department. Personal data must not be stored on this device indefinitely and must be transferred to the college network as soon as possible. Removable devices must be cleared of all personal data after use.

Where staff are approved to use a personal device for college functions, no college personal data will be stored or processed directly on the device. Only college approved remote access will be used to access and process the college's personal data. This refers to personal data directly held within the college's systems and on third-party sites, such as awarding body portals.

Staff working spaces and offices will be kept locked when unattended and steps will be taken to ensure all hard copies of personal data are locked away. Where appropriate, key safes will be used to ensure lockable areas remain secure. Consideration will be given to door security systems such as key pads in multi-occupied rooms to prevent unauthorised access.

Staff will take particular care when working at home or other offsite locations, ensuring steps are taken to minimize the risk of data loss or theft of college devices.

7. DISCLOSURE

Disclosure of personal data will be done with the utmost care and attention. Staff will ensure they only disclose personal data to authorised persons and third parties using approved security measures for transmitting data, such as encryption or password protection. Staff will verify the identity of those seeking information before disclosure. Care will be taken to avoid casual disclosure either verbally in spaces where other individuals are present or via hard copies left unattended.

Request by other public bodies, including the police, must meet the requirements for lawful processing. The police must be able to demonstrate that they require the information in pursuit of a criminal investigation.

Data relating to a learner's course, their performance and attendance can be disclosed to a sponsor as part of the learner's contract with the college and this will be communicated to the learner on their application/enrolment form. The college reserves the right to contact learners' parents/guardians or any age where there is a need related to their college studies. This will be communicated to the learner on their application/enrolment form. A learner can request information is not shared with their parent/guardian via the Head of Learner Services.

Where the college shares data with third parties, sharing and or processing agreements will be signed by both parties to demonstrate compliance with the UK GDPR/DPA 2018.

Any unauthorised disclosure of personal data will be investigated under the terms of the disciplinary policy and may be considered gross misconduct in some cases.

8. BREACH

Any breach of the GDPR must be notified to the DPO as soon as possible within 24 hours. Notification will be via the Information Security Incident portal on the intranet. The DPO will follow up with appropriate action. All breaches will be reviewed by the Information Governance Group and added to an on-going risk register where necessary.

Where applicable, the DPO will notify the ICO (Information Commissioner s Office) with details of the breach and steps taken to mitigate within 72 hours of notification.

Where there is a serious breach to data protection, the incident must be notified instantly and verbal notification is satisfactory. For serious breaches identified outside of core business hours (8.30am-5pm), notification must be given via an emergency telephone number, which is stated in the associated procedures.

9. SPECIAL CATEGORY & CRIMINAL CONVICTIONS DATA

The GDPR gives special consideration to data that falls under what it terms 'special categories.' It relates to data that falls into the following: race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometric ID data, health, and sex life/sexual orientation.

Where applicable, the college will seek data subject consent to

10. RESPONSIBILITIES

Governing Body	Ultimately responsible for the implementation of this policy
DPO	Review this policy and ensure related registers are kept up to date
Information Governance Group Members	Assist with the review of the policy and related procedures
Asset Owners	Keeping a record of personal data assets within their area and informing the DPO of any amendments
Staff	Comply with