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**
Published on:	**Website** **Staff Portal** **Learner Portal**

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 Essentials requirements Updated following COVID and new way of working remotely

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: -

- ensure that learners and staff are fully aware of their personal responsibilities for protecting themselves and the college's information assets in accordance with College or any external organisation's guidelines;
- prevent data loss and criminality;
- maintain and improve its reputation and meet its legal obligations and strategic business and professional goals; and
- protect itself from any financial loss arising from security breaches.

PURPOSE & SCOPE

This framework applies to all learners and members of staff, including individuals conducting work at or for the College *(referred to in this policy as users)* who are authorised to have access to College ICT resources and/or handle Coleg Gwent information.

For the purpose of this framework, Coleg Gwent ICT resources *(whether they are located on College premises or elsewhere)* include all: -

- hardware (physical & virtual); such as desktops, servers, or mobile devices;
- peripherals; such as monitors, keyboards, external hard drives, and printers;
- networks; such as shared drives, Wi Fi and telecommunications networks and
- systems; such as email and the data associated with systems.

For the purpose of this framework, Coleg Gwent information includes all: -

- electronic formats; and
- hardcopy formats.

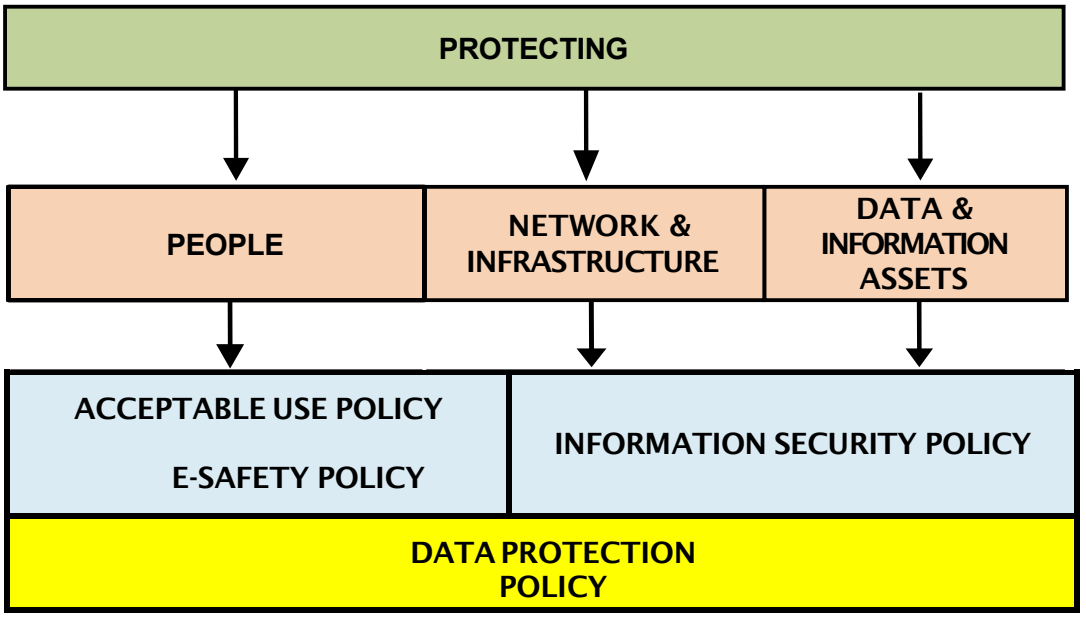
STRUCTURE

The framework is designed around a series of policies aimed at protecting: -

PEOPLE: ensuring that learners, staff, and others who access college ICT facilities remain safe whilst doing so.

NETWORK & INFRASTRUCTURE: ensuring that technical infrastructure and physical assets are secure from theft, damage, unauthorised access, or malicious attack.

DATA & INFORMATION ASSETS: ensuring that all the information that the College collects, processes, and stores is held securely and that the risk of unauthorised access or inappropriate disclosure is minimised.



RESPONSIBILITIES

The Director of ICT is responsible for defining, reviewing, and publishing this framework and for providing guidance and advice in support of it.

All managers are responsible for ensuring that staff and learners within their area of responsibility act in accordance with these policies and established procedures.

All users of Coleg Gwent ICT resources and individuals that handle Coleg Gwent information are expected to have proper awareness of and observe the policies within this framework, both during and, where appropriate, after their time at the College and to act in a responsible and professional way.

Each individual is personally accountable for their behaviour and may be held liable for any breaches of these policies.

REPORTING CONCERNS AND INCIDENTS

The College will ensure that adequate incident reporting is maintained which will detail all incidents which are deemed to have breached the policies included within this framework.

The reporting will contain:

- the nature of the incident;
- details of investigations carried out into the cause of the breach; and
- actions required to reduce the risk of re-occurrence

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 framework and any breach of these policies may lead to:

- disciplinary action in line with college policies;
- withdrawal of a user's right to access Coleg Gwent ICT resources;
- remedial action to resolve any policy contravention; and
- where appropriate, disclosure of information to law enforcement and regulatory agencies

REVIEW, DEVELOPMENT AND DISSEMINATION

The framework, and supporting policies, shall be reviewed, and updated on an annual basis to ensure that they:

- remain operationally fit for purpose;
- reflect changes in technologies;
- are aligned to industry best practice; and
- support continued regulatory, contractual, and legal compliance

The framework, and supporting policies, will be accessible through the staff intranet, the learner portal, and the College website.

LAWS PERTINENT TO THE FRAMEWORK

The framework is to be read in the context of the following legislation:

- The Copyright, Designs and Patents Act (1988);
- The Computer Misuse Act (1990);
- The UK General Data Protection Regulation
- The Data Protection Act (2018);
- The Regulation of Investigatory Powers Act (2000);
- The Freedom of Information Act (2000);
- The Equality Act (2010);
- The Privacy and Electronic Communications Regulations (2003);
- The Environmental Information Regulations (2004); and
- The Digital Economy Act (2017)

FEEDBACK

Coleg Gwent welcomes all constructive feedback on the policies included within this framework. If you would like further information, or wish to send us your comments then please contact Hazel Gunter, PA to the Vice Principal (Resources & Planning) via email at Hazel.Gunter@coleggwent.ac.uk

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 Coleg Gwent users.

- Users must comply with the regulations and policies that are applied by bodies external to the College in respect of ICT resources, including but not restricted to JANET (Joint Academic Network).

- Staff and learners are issued with a Coleg Gwent email address therefore; all college-related emails should be sent via the user's official college email address e.g. joebloggs@coleggwent.ac.uk or 10101010@coleggwent.ac.uk.

- Personal use of ICT resources should not interfere with employees' work duties or learners'

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 example to Wi-Fi issues, these areas can be used on a temporary basis for the duration of the lesson/meeting, but the data must be moved to a backed-up area immediately after.

- Moving or relocating ICT resources on college premises without seeking approval beforehand from the ICT department.

- Using personal devices or removable storage devices (such as USB sticks) for college purposes without seeking approval beforehand from the ICT department.

3. ACCEPTABLE PRACTICES – INFORMATION SECURITY

- Accidental loss or theft of Coleg Gwent ICT resources and /or Coleg Gwent information is classified as a security incident and must be reported immediately.

- Users are responsible for logging out of / or locking their PC, laptop, tablet etc. when they leave their desk / study area.

- Users should store Coleg Gwent information *(electronic format*) on secure storage areas e.g. Coleg Gwent network, Coleg Gwent systems, Coleg Gwent OneDrive, and encrypted USB pens. Coleg Gwent information must not be stored on a user's privately-owned hardware device or personal 'Cloud' service account.

- Users should store Coleg Gwent personal/sensitive information *(hardcopy format*) in secure storage areas e.g. cupboards and rooms with physical access controls.

- Mobile storage devices (USB pens, removable hard drives etc.) must only be used with prior approval from the ICT department. Only Coleg Gwent authorised mobile storage devices, with encryption software applied, should be used to hold personal or sensitive information. Personal information should not be kept on these devices indefinitely and must be transferred to the college network as soon as possible.

- Multi-factor authentication (MFA) will be standard policy (where the software allows for it) for users to access the college software when outside of the college's premises and network

- Requests to take ICT resources 'off-site' (pc's, projectors etc.) must be submitted to the Director of ICT for approval via the line manager.

- Requests for staff laptops must be submitted to the Director of ICT for approval via the line manager. Approval will also act as approval to move laptops 'off-site'.

- 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 or ought to know that they should have no access, is unacceptable.

- Users should ensure that casual disclosure of personal and confidential data does not take place e.g. leaving information on MFD's / printers, or by allowing unauthorised users to view information on smartboards and monitors.

- Coleg Gwent information containing personal and confidential data must be kept securely and destroyed in a confidential manner, in line with the college's Data Protection Policy.

- It is college policy to use encryption software when personal or sensitive information is being sent to third parties. Where third party limitations exist that do not allow for encryption, password protection may be used. This is only to be used where no other alternative exists to allow for the safe transfer of data and the password must be communicated to the third party via a different communication type from the data.

- Password protection must be used if staff are sending personal or sensitive information to a member of the Coleg Gwent community. Good practice is to transmit the password via a different means to the information itself e.g. email a file, but telephone the recipient with the password details.

4. EXEMPTIONS FROM UNACCEPTABLE USE

There are a number of legitimate college activities that may be carried out using Coleg Gwent ICT resources that could be considered unacceptable use. For example, research involving defamatory, discriminatory, or threatening material, the use of images which may depict violence, the study of hate crime, terrorism related material or research into computer intrusion techniques. In such circumstances, advice should be sought from the Director of ICT.

5. REPORTING CONCERNS AND INCIDENTS

All concerns and incidents must be reported immediately via the appropriate reporting channel *(refer to page 2)*.

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.

If a user identifies themselves as a member of staff or learner at the College, this has the potential to create perceptions about the College to a range of external audiences. Posting personal statements of a defamatory or offensive nature regarding Coleg Gwent, its learners or staff will be dealt with under the relevant disciplinary procedure.

Staff and learners will be held personally liable for activity or material published on social networks that compromise themselves, their colleagues and/or the College.

3. SOCIAL NETWORK RELATIONSHIPS

To ensure professional boundaries are maintained staff must use caution if they are 'friends' with colleagues.

Under no circumstances should staff 'friend' learners on these social media platforms (including but not limited to Facebook, Twitter, TikTok). All communication between staff and learners must be done through college approved platforms such as Teams or CG Connect.

In respect to being a 'friend' with a learner, extreme caution must be used and normally this would only happen for purely educational purposes that have been sanctioned by a line-manager.

4. SOCIAL NETWORKS & LEARNER PARTICIPATION

Staff are only permitted to use college approved platforms such as Teams or CG Connect for learner participation in course activities.

5. SOCIAL NETWORKS AND REFERENCE TO COLEG GWENT

Coleg Gwent have a social media presence approved and monitored by Marketing. No other sites representing the Coleg Gwent brand must be set up. Where it is deemed needed to set up a site, Marketing must be informed for approval.

Coleg Gwent retains the right to ownership of any social media profile that references the Coleg Gwent name. Social networks that identify themselves as Coleg Gwent will be monitored by the college and any inactive, inaccurate, or negative presence will be removed.

6. WHATSAPP

The use of WhatsApp between staff and learners or parents is only permitted where the learners partake in a trip or visit as part of their course for safeguarding purposes. Lists of who is on the group must be left with the SA and deleted once the trip has passed.

7. PRIVACY SETTINGS

Staff and learners should review their access and privacy settings for any social networks to control, restrict and guard against who can access the information on those sites. Staff and learners must be aware that social networks are a public forum. Users should not assume that their entries on social networks will remain private e.g. what starts as a private post could be

made public through onward transmission.

8. IDENTITY THEFT

To avoid identity theft, staff and learners should refrain from publishing any personal or sensitive information e.g. date of birth, home address, telephone number or any information related to personal bank accounts.

Individuals should never disclose any username or password to a third party e.g. Coleg Gwent ICT staff or in response to people saying that they are representatives of a banking institution.

Individuals should be aware of potential phishing attempts used to harvest their personal data and not click suspicious links.

9. CYBER BULLYING

Bullying is not limited to the workplace/college and individuals must be aware that technology can be used to support deliberate, repeated, and hostile behaviour by an individual or group. Bullying in any form will not be tolerated and any concerns or incidents must be reported.

10. E-MAIL

Email attachments and embedded links must be reviewed with caution before they are opened. Corrupt emails are high-risk sources for identity theft and introducing viruses into a PC, laptop, smartphone, and network.

Users must not use their Coleg Gwent email address for personal online activity e.g. using it as a secondary contact for a shopping account.

Email can be used in legal and contractual proceedings in the same way as hard copy documentation. Deletion from a user's mailbox does not mean that the email is permanently removed and all emails should be treated as potentially retrievable.

11. INTERNET

It is very easy to make copies of materials on the Internet. But remember that images, text and audio or video clips belong to someone. There are rules about copying other people's material. This is called the law of copyright. If you copy other people's material from the internet without permission, you are breaking the law. This is called copyright infringement, and you could be taken to court, fined and paid compensation to the copyright owner.

Individuals should never do on-line banking, shopping, or access sensitive data on public Wi Fi networks, including accessing the college's remote desktop system.

The College has a duty of care to its learners and staff and must protect its own image and reputation. Therefore, the college applies Internet Content Filters to protect against harmful exposure to content on the Internet. If any individual inadvertently accesses inappropriate material, they should immediately inform their Safeguarding Officer.

12. PREVENT MONITORING

The College has a statutory duty to engage with the government's Prevent agenda, to prevent individuals from being drawn into terrorism. The Internet plays a huge role in the radicalisation of people, and we monitor who is accessing or trying to access harmful content. This information will be passed onto law enforcement agencies if required.

13. USE OF IMAGES AND VIDEO

The use of images or photographs is popular in teaching and learning and should be encouraged where there is no breach of data protection, copyright, or other rights of another person. If learners and/or staff are being photographed, audio recorded or filmed for college related activity, then consent must be sought beforehand.

14. EDUCATION AND TRAINING

The pace of change with technology means new E-Safety concerns are discovered almost weekly. The college cannot eliminate all risks for staff and learners, but it will support staff and learners to stay safe through regular training and awareness raising initiatives.

15. FUTURE DEVELOPMENTS

Technology is a fast-changing landscape, and new technologies emerge regularly. Coleg Gwent encourages individuals to engage with new and emerging technologies. If anyone is unsure or is in doubt about whether they should be using new technology in their line of work, please speak to the Director of ICT to discuss its possibilities and obtain permission before use.

Where new technologies use personal data, a Data Protection Impact Assessment (DPIA) must be completed to assess the risk to personal data

16. REPORTINGCONCERNSAND INCIDENTS

Individuals are expected to seek help where they are worried or concerned, or where they believe an E-Safety incident has taken place involving them or another member of the college community (*refer to page 2*).

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. 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.

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.

PURPOSE AND SCOPE

The purpose of this policy is to ensure that Coleg Gwent (The College) meets its obligations in relation to the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). It covers all personal data held and processed by Coleg Gwent, its processors, joint controllers, and contractors. Personal data is processed in relation to Coleg Gwent's corporation members, employees, learners, partners, suppliers, and other users as a normal part of its day-to-day business.

It is the intention of Coleg Gwent to comply with the terms of the UK GDPR/DPA 2018. The College will ensure that the interests of its employees and learners are safeguarded by regularly reviewing its policy and taking account of Codes of Practice and other advice issued by the Information Commissioner's Office. Coleg Gwent will also take account of the wider legal framework introduced by the Regulation of Investigatory Powers Act 2000, the Human Rights Act 1998, the Freedom of Information Act 2000, the Privacy and Electronic Communications Regulations 2003, the Computer Misuse Act 1990 and the Crime and Disorder Act 1998.

Coleg Gwent and all staff or others who process or use personal information must ensure that they follow the Data Protection Principles at all times. To ensure that this happens, Coleg Gwent has developed this Data Protection Policy and associated financial control procedures.

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by Coleg Gwent from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

Coleg Gwent acknowledges that the Corporation may be held liable for criminal offences under the UK GDPR and DPA 2018.

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 collection, alteration, storage, erasure
Controller	The body that determines the purpose and means of processing of personal data
Processor	The body that processes personal data on behalf of and under instruction from the controller
Third Party	A person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
Consent	any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her
Personal Data Breach	Breach of security leading to accidental or unlawful loss, alteration, access/disclosure, or personal data

1. PRINCIPLES

Coleg Gwent is committed to processing personal data in accordance with the following principles. Personal data shall be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant, and limited to what is necessary in relation to the purposes of processing;
- Accurate;
- Stored in an identifiable form for no longer than is necessary;
- Processed in a manner that ensures security

The controller is also responsible for demonstrating compliance with the principle of accountability. This requires the college to evidence its compliance with the legislation. The college has appropriate and effective measures in place to ensure it complies with the principles. Policies, procedures, and training are available to all staff to familiarise themselves with this legislation.

2. LAWFUL PURPOSES

All data processed by Coleg Gwent, its processors and other third parties must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task, or legitimate interests. This is set out in the college's Register of Legal Bases.

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 Gwent Financial Procedures Manual. Formal records may only be destroyed with the appropriate authority.

6. SECURITY

Data protection and information security will be reviewed regularly and be placed as a recurring item on senior management meetings. Where appropriate, it will be a component of the corporate risk register.

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.

Where a disclosure is requested in an emergency, staff should make a careful decision as to whether to disclose, considering the nature of the information being requested and the likely impact on the subject of not providing it. All disclosure requests from external parties must be approved by the Data Protection Officer. If this is not possible due to the urgency of the information, the DPO should be informed at the earliest opportunity of the details.

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 process their special category data. However, it is sometimes necessary to process this data to ensure the college remains a safe place for everyone or to operate other college policies such as the Safeguarding Policy or the Equality and Diversity policy. In these situations, the college relies on another legal basis for processing.

The college will ask for information related to health conditions to ensure safety measures are taken, for example where staff and learners will be in contact with livestock or chemicals that may aggravate a known condition of the data subject.

To process data relating to criminal convictions, the college needs a specific legal basis. This is set out in the Register of Legal Bases.

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 this policy and any associated procedures. Keep up to date with relevant training. Inform the DPO of any activity contrary to this policy
Learners	Comply with the policy and any associated procedures. Inform their tutor of any activity contrary to this policy. Attend any induction sessions related to this policy
Third Parties/Contractors	Sign the College's processing or sharing agreement agreeing to abide to this policy
Estates Staff	Review and management of the archive and related procedures

Do's and Don'ts for Staff

Do….

- Always think of how your day-to-day actions could impact on data protection by always following the data protection principles
- Keep up to date with your data protection and cyber security training
- Familiarise yourself with the financial control procedures linked to data protection (17.7, 17.9 & 17.10) which can be found on the staff portal.
- Only use and collect personal data that is relevant to your purpose and make sure you have a legal basis to process the data
- Notify of any potential data protection breaches using the reporting tile on the staff portal
- Take care when talking about personal data in public areas to make sure people cannot overhear you
- Contact the DPO (DPO@coleggwent.ac.uk) if you are unsure of anything in this policy

Don't…

- Put paperwork containing personal data in the normal bin – use the confidential waste sacks
- Leave personal data unattended. Make sure to lock it in cupboards, lock PC screens
- Download personal data onto personal devices – use the remote desktop to access all personal data
- Give out personal data to unauthorised people. Verify identities before all disclosures.
- Share passwords.
- Use simple passwords such as 1234567 or qwerty

Remember…

- Failure to adhere to this policy could result in disciplinary action and may be classed as gross misconduct
- Personal data relates to ALL living individuals that can be identified directly or indirectly by the data – this includes photos, videos, voice recordings as well as things like name, address, ID number.
- Everyone is accountable and has a responsibility to protect personal data
- Personal data must not be stored on removable devices indefinitely and must be transferred to the college network as soon as possible. Prior approval must be sought from ICT.

The Principles -

Personal Data shall be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant, and limited to what is necessary in relation to the purposes of processing
- Accurate
- Stored in an identifiable form for no longer than is necessary
- Processed in a manner that ensures security