Information Security Framework

Incorporating:

Acceptable Use Policy
E-Safety Policy
Information Security Policy

Date Equality Impact Assessment Completed:	19-09-2016
Approved By:	CMT
Date Approved:	27-09-2016
Author:	Head of ICT, Diane Clark
Review Date:	01-08-2017

Published on:	Website (✓)	Intranet (✓)	Learner Portal (✓)
	28-10-2016	28-10-2016	28-10-2016

Available in large font and other formats on request

This copy may be out of date if printed

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: -

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 IT resources and/or handle Coleg Gwent information.

For the purpose of this framework, Coleg Gwent IT 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.

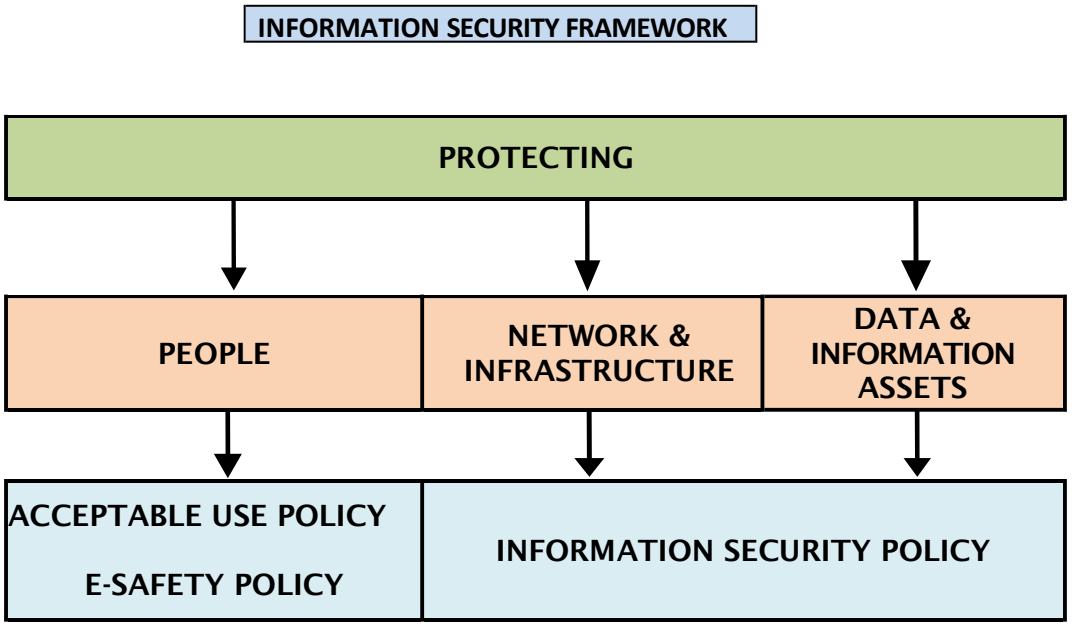
STRUCTURE

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

PEOPLE: ensuring that learners, staff and others who access college IT 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 Head 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 IT 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 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:

INFORMATION SECURITY FRAMEWORK

Policy	Reporting Manager	Name
Acceptable Use	Head of ICT	Diane Clark
E-Safety	Safeguarding Officers	BGLZ: Julie Hope Crosskeys: Bill Mason Newport: June Bridgeman Pontypool & Usk: Sian Hughes
Information Security	Data Protection Officer Head of ICT	Anna Lebar-Hill Diane Clark

MONITORING

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 Data Protection Act 1998 and where this is permitted under the Regulation of Investigatory Powers Act 2000 (and associated regulations) for the purpose of:

a) preventing or detecting criminal activities;
b) investigating or detecting unauthorised use of the College's IT resources;
c) ascertaining compliance with regulatory or self-regulatory practices or procedures and standards; and
d) 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 IT resources. However, where, for example, there are reasonable grounds to suspect an instance of unacceptable use of any IT resources, or where a legitimate request is made by the police or other authority, permission may be granted for the monitoring or investigation of an individual's use of College IT facilities. This may include the monitoring of email and use of the internet.

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 IT 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 law enforcement agencies

involved in the prevention and detection of crime and to no other third party.

CONSEQUENCES OF NON- COMPLIANCE

Non-compliance with the framework and any breach of these policies may lead to:

a) disciplinary action in line with college policies;
b) withdrawal of a user's right to access Coleg Gwent IT resources;
c) remedial action to resolve any policy contravention; and
d) 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 (1998);
- The Computer Misuse Act (1990);
- The Data Protection Act (1998);
- The Regulation of Investigatory Powers Act (2000);
- The Freedom of Information Act (2000);
- The Privacy and Electronic Communications Regulations (2003);
- The Environmental Information Regulations (2004); and
- The Digital Economy Act (2010)

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 & Financial 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 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:

a) acceptable use of Coleg Gwent IT resources;
b) unacceptable use of Coleg Gwent IT resources;
c) 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 – IT RESOURCES

- Users are issued with a username and password which must be used to authenticate and gain access to IT 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.

- Users are responsible for all activity that takes place under their username and must not allow anyone else to access IT resources using their username and password.

- Users must comply with the regulations and policies that are applied by bodies external to the College in respect of IT 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 IT 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, malware or ransomware must be reported to the ICT department immediately.

- Any Coleg Gwent IT 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 – IT RESOURCES

- Coleg Gwent IT resources must not be used for the download, creation, manipulation, transmission or storage of:
    - any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
    - unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others;
    - unsolicited "nuisance" emails;
    - material which is subsequently used to facilitate harassment, bullying and/or victimisation;
    - material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation;
    - material with the intent to defraud or which is likely to deceive a third party;
    - material which advocates or promotes any unlawful act;
    - 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;
    - 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 IT resource.

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

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

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

- Using Coleg Gwent IT 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.

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

3. ACCEPTABLE PRACTICES – INFORMATION SECURITY

- Accidental loss or theft of Coleg Gwent IT 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 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 be used only in situations when network connectivity is unavailable or there is no other secure means of transferring data. Only Coleg Gwent authorised mobile storage devices, with encryption software applied, should be used to hold personal or sensitive information.

- Requests to take IT resources 'off-site' (loan of laptops, desk top printers etc.) must be submitted to the Head of ICT for approval.

- Coleg Gwent IT 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 / classlists overnight in cars.

- 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.

- Encryption software must be used if staff are sending personal or sensitive information to an external or third party.

- 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 IT 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 Campus Director or Head 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, 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. 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

It is not compulsory for learners to participate in messaging or social network groups using their personal profiles. Staff need to be aware of this when planning to use these technologies as part of their teaching or communication plans.

5. SOCIAL NETWORKS AND REFERENCE TO COLEG GWENT

Staff who create a social media presence relating to Coleg Gwent (e.g. a Facebook group or YouTube channel) must inform the Head of Marketing & Communications and follow the approved procedure.

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. 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.

7. 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 3rd party e.g. Coleg Gwent ICT staff or in response to people saying that they are representatives of a banking institution.

8. 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.

9. E-MAIL

Email attachments should be opened with care unless you have absolute confidence in its origin. Opening corrupt email attachments is one of the most likely sources of introducing a virus into a PC, laptop, smartphone and network.

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.

10. INTERNET

It's 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're breaking the law. This is called copyright infringement and you could be taken to court, fined and have to pay compensation to the copyright owner.

Individuals should never do on-line banking, shopping or access sensitive data on public Wi Fi networks.

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.

11. 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.

12. 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.

13. EDUCATION AND TRAINING

The pace of change with technology means that new E-Safety concerns are discovered on an almost weekly basis. 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.

14. FUTURE DEVELOPMENTS

Technology is a fast changing landscape and new technologies emerge on a regular basis. Coleg Gwent encourages individuals to engage with new and emerging technologies. If any individual is unsure or is in any doubt if they should be using a new technology in their line of work, please speak to the Head of ICT to discuss its possibilities and obtain permission before use.

15. REPORTING CONCERNS AND 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 or the matter may be resolved internally depending on the seriousness of the incident. 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 IT 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, 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 IT 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 IT resources must be effectively managed and kept secure from theft and damage. Redundant Coleg Gwent IT 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 IT 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 on all of the College's infrastructure, systems and processes on a regular basis in order 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.

7. EDUCATION AND TRAINING

All users of College IT resources, and individuals that handle information should complete information security awareness training.

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.