Audit & RIsk Committee

Wednesday 11 March 2026, 4pm by Teams

Agenda No: 5

Title of Paper	Policies
Presented by:	Senior Leadership Team
Action:	For Approval and Recommendation to the Board
Status:	PUBLIC once approved
Linked To:	**Organisational Governance**
KPI(s)	n/a
Strategic Theme	All
Strategic Enabler	All
Risk Category	Finance / Staff / Students / Reputation / Infrastructure / Regulatory

Purpose / Executive Summary:
Four key policies have been reviewed and updated and are attached. These are:

- Records Management Policy (required under the Public Records (Scotland) Act 2011)
- Data Protection Policy (necessary for UK GDPR & Data Protection Act 2018 accountability requirements)
- Business Continuity Policy
- Business Continuity Plan

Recommendations:
The Audit & RIsk Committee are requested to consider the content of the policies and approve their recommendation to the Board for final approval. Corporate Development Committee have also had oversight of the policies.

Implications:	
Financial	There are no direct financial implications associated with these policies.
Student Experience	There are no direct student experience implications associated with these policies.
People	There are no significant people implications associated with these policies.
Legal	Policies are designed to adhere to current legal instruments.
Reputational	Lack of governance in data protection/records management could lead to significant reputational damage, due to the College having large volumes of sensitive data which it is obliged to protect.
Community/ Partnership impact	There are no direct community / partnership implications associated with these policies.
Environment	Policies discourage the creation or retention of large volumes of paper files, and therefore they are helpful for the environment.
Equalities	There are no significant equalities implications associated with these policies.

WEST COLLEGE SCOTLAND

Records Management Policy

Approved:

March 2023

Date for Review:

March 2026

Records Management Policy

Quick Guide

Purpose

The purpose of this policy is to demonstrate the importance of managing records effectively within the College and to act as a mandate for the support and delivery of records management policies, procedures, and initiatives across the organisation.

General Principles:

- Records must be held in compliance with all applicable legal, regulatory, and contractual requirements.
- Records must not be held for any longer than required.
- The protection of records in terms of their confidentiality, integrity and availability must be in accordance with their security classification.
- Records must always remain retrievable in line with business requirements.
- This policy relates to all teams and business areas of WCS and all records created by our employees.
- It relates to the management of records as an internal, facilitative function of the organisation and covers the records created by the organisation, about its activities.
- It applies to all records regardless of format or medium, including paper, electronic, audio, visual, microform and photographic.

Record Types and Guidelines:

To assist with the definition of guidelines for record retention and protection, records held by WCS are defined with retention periods in the WCS Retention and Disposal Schedule.

Record Disposal Methods:

- **Confidential Destruction** Cross-cut shredding or incineration, either internally or by an approved third-party contractor.
- **Deletion** – deleting documents and records from electronic systems.
- **Recycling** – non-sensitive information can be recycled by a reputable company, into a useable product.
- **Transfer to Archive** – records of enduring value selected for permanent retention should be transferred to archive.

History of Amendments

Date	Version/Pages/ Sections Affected	Summary of changes
March 2024	All	Transferred to new format and updated

Policy Statement
It is the policy of WCS to maintain authentic, reliable, and useable records, which can support business functions and activities for as long as they are required. WCS is therefore committed to the operation and continuous improvement of effective records management policies and procedures.
Equality Statement
The College is committed to providing equal opportunities to ensure its students, staff, customers and visitors are treated equally regardless of gender reassignment, race, religion or belief; disability; age; marriage and civil partnerships; pregnancy and maternity; sexual orientation; sex. Please note this document is available in other formats, to request another format please email info@wcs.ac.uk

Contents

1. Introduction

The Public Records (Scotland) Act 2011 places an obligation on named authorities in Scotland to produce a records management plan which sets out their arrangements for the effective management of all records.

FE Colleges are not named as authorities in the schedule of the Act, but it is nevertheless good practice to manage records formally and efficiently.

2. What is Records Management?

Records management can be defined as the process whereby an organisation manages its records, whether created internally or externally and in any format or media type, from their creation or receipt, through to their destruction or permanent preservation.
Records management is about placing controls around each stage of a record's lifecycle:

- at the point of creation (through the application of metadata, version control and naming conventions),
- during maintenance and use (through the management of security and access classifications, facilities for access and tracking of records),
- at regular review intervals (through the application of retention and disposal criteria),
- and ultimate disposal (whether this be recycling, confidential destruction or transfer to the archive branch for permanent preservation).

By placing such controls around the lifecycle of a record, we can ensure they demonstrate the key attributes of authenticity, reliability, integrity, and accessibility, both now and in the future.

Through the effective management of the organisation's records, West College Scotland (WCS) can provide a comprehensive and accurate account of its activities and transactions. This may be achieved through the management of effective metadata as well as the maintenance of comprehensive audit trail data.

We retain records that provide evidence of our functions, activities, and transactions, for:

- Operational Use – to serve the purpose for which they were originally created, to support our decision-making processes, to allow us to look back at decisions made previously and to learn from previous successes and failure, and to protect the organisation's assets and rights.
- Internal and External Accountability – to demonstrate transparency and accountability for all actions, to provide evidence of legislative, regulatory, and statutory compliance and to demonstrate that all business is conducted in line with best practice.
- Historical and Cultural Value – to protect and make available the corporate memory of the organisation to all stakeholders and for future generations.

3. Why is Records Management Important?

Information and records are a valuable corporate asset without which we would be unable to carry out our functions, activities, and transactions, meet the needs of our stakeholders, and ensure legislative compliance.

The benefits of implementing records management systems and processes include:

- Improved information sharing and the provision of quick and easy access to the right information at the right time.
- The support and facilitation of more efficient service delivery.
- Improved business efficiency through reduced time spent searching for information.
- Demonstration of transparency and accountability for all actions.
- The maintenance of corporate memory.
- The creation of better working environments and identification of opportunities for office rationalisation and increased mobile working.
- Risk management in terms of ensuring and demonstrating compliance with all legal, regulatory, and statutory obligations.

- The meeting of stakeholder expectations through the provision of excellent quality services.

4. General Principles

There are several key general principles that must be adopted when considering record retention and protection policy. These are:

- Records must be held in compliance with all applicable legal, regulatory, and contractual requirements.
- Records must not be held for any longer than required.
- The protection of records in terms of their confidentiality, integrity and availability must be in accordance with their security classification.
- Records must always remain retrievable in line with business requirements.
- This policy relates to all teams and business areas of WCS and all records created by our employees.
- It relates to the management of records as an internal, facilitative function of the organisation and covers the records created by the organisation, about its activities.
- It applies to all records regardless of format or medium, including paper, electronic, audio, visual, microform and photographic.

5. Roles and responsibilities

All managers and heads of department have responsibility for records management within their area. They should be familiar with this policy and ensure that their area of responsibility complies with the policy. Organisational core systems should be used for records storage, wherever possible. The following table is indicative, but not exhaustive.

Departmental Area	**Responsible Officer**
The Board	Secretary, Board of Management
Executive Area	Executive Team
Organisational Development & HR	Head of OD and HR
Enterprise and Employability	Head of Enterprise and Employability

Campus Operations	Head of Campus Operations
Engineering	Head of Engineering Technologies
Student Academic Skills Development	Head of Academic and Skills Development
Language, Business and Leisure	Head of Languages, Business and Leisure Industries
Health, Wellbeing and Care	Head of Health, Wellbeing and Care
Access and Progression	Head of Access and Progression
Business Development	Head of Business Development
Construction and Building	Head of Construction and Building Services
Finance	Head of Finance
Student Services	Head of Student Services
Creative and Digital	Head of Creative and Digital Industries
Information Technology	Head of Information Technologies

6. Record Types and Guidelines

To assist with the definition of guidelines for record retention and protection, records held by WCS are defined with retention periods in the WCS Retention and Disposal Schedule

This policy applies to all teams as a minimum; however, teams may have additional arrangements documented.

7. Media Selection

The choice of long-term storage media must consider the physical characteristics of the medium and the length of time it will be in use. Where records are legally (or practically) required to be stored on paper, adequate precautions must be taken to ensure that environmental conditions remain suitable for the type of paper used. Where possible, backup copies of such records may be taken by methods such as scanning or digitisation. Regular checks must be made to assess the rate of deterioration of the paper and action taken to preserve the records if required.

For records stored on electronic media such as tape, similar precautions must be taken to ensure the longevity of the materials,

including correct storage, and copying onto more robust media if necessary. The ability to read the contents of the tape (or other similar media) format must be maintained by the keeping of a device capable of processing it. If this is impractical an external third party may be employed to convert the media onto an alternative format.

8. Record Retrieval

There is little point in retaining records if they are not able to be accessed in line with business or legal requirements. The choice and maintenance of record storage facilities must ensure that records can be retrieved in a usable format within an acceptable period. An appropriate balance should be struck between the cost of storage and the speed of retrieval so that the most likely circumstances are adequately catered for. Records should be kept on college core systems, where practicable.

Core Systems:
Microsoft 365
OneDrive
SharePoint
MS Teams
Moodle
UNITe
CIVICA
Evolve
iTrent
and other officially procured departmental software tools.

Staff should not store records or personal data on pen drives, removable media, social media apps, or messaging services (WhatsApp, Telegraph etc.).

9. Record Destruction

Once records have reached the end of their life, they must be securely destroyed in a manner that ensures that they can no longer be used.

10. Disposal Methods

There are four methods for the disposal of information:

- **Confidential Destruction** – official information should be destroyed in such a way that it cannot be reproduced by a third party and is completely illegible. This may be achieved through cross-cut shredding or incineration, either internally or by an approved third-party contractor.
- **Deletion** – deleting documents and records from electronic systems.
- **Recycling** – non-sensitive information can be recycled by a reputable company, into a useable product.
- **Transfer to Archive** – records of enduring value selected for permanent retention should be transferred to archive.

Both paper and electronic records should be regularly reviewed. Please note that any information currently subject to a Freedom of Information or Data Protection subject access request should be retained until at least 3 months days after the request has been fulfilled.

For information on all current requests, please contact dpo@wcs.ac.uk or foi@wcs.ac.uk.

10.1. Confidential Disposal of Official Physical Waste

Any information that WCS collects, stores, processes, generates or shares to deliver services and conduct business will be considered official material, with a security classification of at least INTERNAL. Some official material will attract a SENSITIVE handling caveat. This classification will apply to information which could have more damaging consequences for individuals or WCS generally if it were lost, stolen, or published in the media.

All official paper waste should be placed within the lockable consoles which are in use in all WCS campuses.

Confidential Waste consoles are emptied regularly, and their contents are shredded offsite. If you find that a console is full, please notify Estates, who will direct you to another one which has capacity. Estates can provide guidance on the location of consoles within buildings and on bulk waste disposal.

Shredders are also available in some buildings. These should be used to dispose of SENSITIVE material or other sensitive material which particularly merits a securer form of destruction. However, most official waste should now be disposed of in consoles rather than shredders. Waste from the shredder bins is disposed of as confidential waste.

If you have multimedia or hardware which requires confidential disposal raise a request through the IT Department. IT will arrange for the collection and disposal of this material.

For bulk disposal of archives waste at other times of the year please log a call via Estates.

A record of destruction should be retained for all material destroyed confidentially. Certificates of destruction are provided by the contractor who uplift waste. These certificates are then stored by Estates.

10.2. Deletion of Electronic Information

When deleting electronic information from systems ensure that any duplicates are also deleted and that you regularly empty the Recycle Bin on your computer desktop.

Emails deleted from Outlook mailboxes are deleted from the Exchange Server after 30 days. The Exchange Server is also backed up to disk for 12 weeks and 13-week-old data is purged.

Hard disk drives and removable media must be security wiped of data before they are disposed of in accordance with the IT Asset Disposal Procedure.

10.3. Disposal of Unofficial Waste (Non Sensitive)

All unofficial material should be placed in the bins available in all WCS buildings. The smaller paper waste recycling bins, which are colour coded green can also be used to dispose of unofficial waste. These sacks and bins will be checked regularly, and their contents disposed of appropriately. Staff should not use confidential waste consoles for the destruction of unofficial material as this is very costly to the organisation.

10.4. Transfer of Records to Archive

Any records of enduring value should be transferred to the College archives, in accordance with WCS's Archiving Arrangements.
Heads of departments are responsible for identifying records which merit permanent preservation on account of their enduring historical, cultural and research value.

11. Record Review

The retention and storage of records must be subject to a regular review process carried out under the guidance of management to ensure that:

- Records are being retained according to the policy .
- Records are being securely disposed of when no longer required.
- Legal, regulatory, and contractual requirements are being fulfilled.
- Records identified and kept for permanent preservation.
- Processes for record retrieval are meeting business requirements
  The results of these reviews must be recorded.

12. Useful Links

- Records Disposal Schedule

  https://intranet.westcollegescotland.ac.uk/teams/odhrportal/GDPR/Records%20Disposal%20Schedule%20Template.docx

- Retention Disposal Schedule
- GDPR Guidance Folder

13. Equality Impact Assessment

The Equality Impact Assessment can be found here

WEST COLLEGE SCOTLAND

Data Protection Policy

Approved:

March 2023

Date for Review:

March 2026

Data Protection Policy

Quick Guide

Purpose

This document outlines West College Scotland's approach to the management of personal data, particularly special category and criminal conviction data processed by the College, as required by the UK General Data Protection Regulation (UK GDPR), Article 9 and the Data Protection Act 2018, Schedule 1, Part 4.

General Principles:

West College Scotland processes special category and criminal conviction data as part of its statutory duties under employment and social protection law, and for reasons of substantial public interest. The College will detail its procedures for compliance with the principles of Article 5 of the UK GDPR, and outline its policies as regards retention and erasure of this data.

GDPR Article 5 Compliance:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

Types of Data:

- **Criminal Conviction Data** - Data processed relating to criminal convictions and offences, or related security measures. The most common processing of this data in the College is when staff are checked for recorded criminal convictions with Disclosure Scotland under the PVG scheme.

- **Special category data**
  - Racial or ethnic origin
  - Political opinions
  - Religious or philosophical beliefs
  - Trade Union membership
  - Genetic and biometric data used to identify an individual
  - Health data
  - Sexual/ sex life data
  - Sexual orientation
  - Protected characteristics not covered above.

History of Amendments

Date	Version/Pages/ Sections Affected	Summary of changes
April 2017	Pages 19/20	Retention details updated
April 2018	Whole document	Revised for implementation of EU GDPR
March 2019	Section 12	Updated to include reference to Subject Access Request Procedure
October 2022	Whole document	Overhaul of content and structure
October 2022	Whole document	Update of legislative references, particularly UK GDPR
October 2022	Whole document	Inclusion of requirements related to DPA 2018, Schedule 1, Part 4: special category and criminal conviction data
February 2024	Whole document	Update and convert to new format

Policy Statement

The UK General Data Protection Regulation (UK GDPR) requires the College to process any personal data in accordance with the UK GDPR Data Protection Principles and ensure that we meet our legal obligations as laid down in Data Protection Law. This Policy has been reviewed to enable the College to comply with the requirements of the UK GDPR and the Data Protection Act 2018.
West College Scotland processes special category and criminal conviction data as part of its statutory duties under employment and social protection law, and for reasons of substantial public interest. The College will detail its procedures for compliance with the principles of Article 5 of the UK GDPR, and outline its policies as regards retention and erasure of this data.

Equality Statement

The College is committed to providing equal opportunities to ensure its students, staff, customers and visitors are treated equally regardless of gender reassignment, race, religion or belief;

disability; age; marriage and civil partnerships; pregnancy and maternity; sexual orientation; sex.

Please note this document is available in other formats, to request another format please email info@wcs.ac.uk

Contents

1. Purpose

This document and associated procedures referred to in this document outlines West College Scotland's approach to the management of personal data, particularly special category and criminal conviction data processed by the College, as required by the UK General Data Protection Regulation (UK GDPR), Article 9 and the Data Protection Act 2018, Schedule 1, Part 4.

2. Policy Statement

West College Scotland processes special category and criminal conviction data as part of its statutory duties under employment and social protection law, and for reasons of substantial public interest. The College will detail its procedures for compliance with the principles of Article 5 of the UK GDPR, and outline its policies as regards retention and erasure of this data.

3. Responsibility for the Implementation of this Policy and Associated Procedures

This policy applies to all College staff processing personal data, special category personal data, protected characteristics data, and criminal convictions data.

4. Definitions

a) Criminal Conviction data

Criminal conviction data is the data processed relating to criminal convictions and offences, or related security measures (UK GDPR, Article 10). The most common processing of this data in the College is when staff are checked for recorded criminal convictions with

Disclosure Scotland under the Protecting Vulnerable Groups (PVG) scheme. Students on work placements may also be Disclosure Scotland checked, for example if their placement is at a nursery or requires them to work with children or vulnerable adults.

b) Special category data is defined by UK GDPR Article 9(1):

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union membership
- Genetic and biometric data used to identify an individual
- Health data
- Sexual/ sex life data
- Sexual orientation

c) Protected Characteristics

Protected Characteristics, as defined under the Equality Act 2010 (Article 4), should be treated as Special Category Data for data processing purposes and include:

- age
- disability
- gender reassignment
- marriage and civil partnership
- pregnancy and maternity
- race
- religion or belief
- sex
- sexual orientation

5. What Laws Apply

Due to the sensitive nature of special category data, protected characteristic data and criminal convictions data, there are a number of laws in place to restrict and manage processing of this information by organisations, including Colleges. Other laws oblige the College to

process such data for specific purposes. The three areas of legislation most relevant at this time are described below. Note that, should any of these legislative vehicles be superseded during the period of this policy, then the most relevant legislation will be deemed to be covered by this policy.

5.1. UK General Data Protection Legislation (UK GDPR)

GDPR is EU legislation which came into force on 25 May 2018. UK GDPR is legislation which came into force in the UK on 31/12/20, due to the UK's exit from the European Union. UK GDPR was created by amendments in the The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

The reason for this legislation is to ensure that the privacy rights of individuals are upheld by organisations, including Colleges, that process personal data. Organisations must only process personal data where it is lawful and fair to do so; be transparent in how they process this data; process the data only for the purpose it was collected; only request the minimum amount of data required for the purpose; ensure the data is accurate, up-to-date and not kept longer than necessary; and is processed using technical and organizational measures that ensures the security of the data.

UK GDPR provides protection to personal data; that is information that relates to a clearly identifiable living individual, for example a student or a member of staff.

UK GDPR supports an individuals' rights in relation to the personal data an organisation, such as a college, processes, including being made aware of how their data is processed; requesting copies of some or all of this information or requesting that their information is changed, updated or deleted; and restricting processing of their data.

Most personal data collected by the College from students and staff is processed on the basis of contract (Article 6(1)(b), or public task (Article6(1)(e)). Most special category and protected characteristics

data is collected by the College on the basis of employment and social protection law (Article 9(2)(b) or substantial public interest (Article9(2)(g)). Criminal convictions data collected by the College is done so in-line with Article 10 of the UK GDPR, which stipulates that processing can only be carried out under the control of official authority, or when the processing meets the requirements of the Data Protection Act 2018 (see below), with appropriate safeguards in place to protect the rights and freedoms of data subjects.

5.2. Data Protection Act 2018 (DPA 2018)

The DPA 2018 enacted the EU GDPR law into UK law and establishes additional safeguards for handling special category and criminal conviction data (Schedule 1, Part 4):

- an appropriate policy document (this document);
- outlining how the controller's procedures comply with the UK GDPR Principles (Article 5) (e.g. Data Protection Policy/Procedure/Guidance)
- outlining the controller's policies on retention and deletion of data, and whether policies are strictly adhered to
- retaining and reviewing policy document(s)
- making this document available to the Information Commissioner's Office upon request.

5.3. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)

The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the UK GDPR. They give people specific privacy rights in relation to electronic communications.

There are specific rules on:

- marketing calls, emails, texts and faxes
- cookies (and similar technologies)
- keeping communications services secure; and

- customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

6. UK GDPR Article 5 Compliance

The College complies with the UK GDPR Principles under Article 5, as outlined in the College Data Policy, and underlying procedural documents which are available on the College intranet.

1. Lawfulness, fairness and transparency
The College will regularly review forms and other methods of gathering data, to ensure that the processing is fair and lawful. The College will be transparent with data subjects and publish privacy notices where appropriate.

2. Purpose limitation
The College will ensure that data is only processed for the purposes listed in the Records of Processing Activity.

3. Data minimisation
The College will not collect or process data for which there is not a listed purpose in the Records of Processing Activity.

4. Accuracy
The College will ensure, wherever possible, that data subjects can access and update their records, to ensure accuracy.

5. Storage limitation
Data will be securely deleted at the end of the listed retention periods. Departmental retention schedules can be found on the College intranet.

6. Integrity and confidentiality (security)
The College will make every effort to ensure the security, integrity and confidentiality of data. See the College IT Security Policy. The College is Cyber Essentials Plus certified.

7. Accountability
The College will keep detailed records relating to compliance and accountability issues and will record these in a version of the Information Commissioner's accountability tracker.

7. Staff Training

The College will ensure all staff are trained in data protection, specifically relating to personal, special category and 'protected characteristics' data and the legislation underpinning this (see Section 3 above). This training will be periodically refreshed and will form part of the induction process for all new staff.

8. Advice for Staff

While all staff will receive training (outlined in Section 5 above), the College recognises that staff may either require specialist advice or assistance where a request for personal and/or College information goes beyond what a reasonable member of staff would consider a normal request for someone in their role.

Staff should, in the first instance, discuss their query with their line manager. Should your line manager be unavailable (e.g. on leave or off ill) you should contact the Data Protection Officer at dpo@wcs.ac.uk for advice as soon as possible.

9. Special Category Data: Lawful bases

Special category and/or 'protected characteristics' staff and student data will be processed by the College for several reasons related to, and not incompatible with, the specified purpose for which it was originally collected (as outlined in the College Privacy Notices).

9.1. Staff

The College processes various types of special category data for employees, including:

- Sickness absence data
- Occupational health data
- Health and safety data
- Disciplinary and grievance procedure data
- Trade Union membership data
- Equality and diversity data
- Protected Disclosure data

Article 6 and 9 lawful bases for all data held by the College are available on the College intranet in the Records of Processing Activities.

9.2. Students

The College processes special category data related to students, including:

- Equality and diversity data
- Counselling data
- Health and safety data
- Safeguarding data
- Personal learning support plans
- Personal escape plans

Article 6 and 9 lawful bases for all data held by the College are available on the College intranet in the Records of Processing Activities.

9.3. Exceptional circumstances

There may be exceptional circumstance where the College may have to share special category or 'protected characteristics' data using a different lawful basis, including but not limited to:

An emergency

For example, where a student or member of staff is in a life-or-death situation, the College may have to share special category data to a paramedic, or other health worker:

- UK GDPR Article 6(1)(d) – vital interests
- UK GDPR Article 9(2)(c) – vital interests

Legal claims

For example, where the College is approached and asked to provide data on staff or students necessary to establish, exercise or defend a legal claim or as evidence for court:

- UK GDPR Article 6(1)(c) – legal obligation
- UK GDPR Article 9(2)(f) – legal claims

10. Criminal Convictions Data: Lawful Bases

The College has a statutory duty to protect children and vulnerable adults, as outlined in the Protection of Vulnerable Groups (Scotland) Act 2007. Where appropriate, the College will conduct criminal convictions checks to ensure that staff in contact with children and vulnerable adults do not pose a threat to their safety.
Similarly, the College will conduct criminal convictions checks to ensure that students undertaking a work placement where they will be in contact with children and vulnerable adults do not pose a threat to their safety.

This means that the College processes staff and/or student criminal convictions data on the following legal bases:

- UK GDPR Article 6(1)(c) – legal obligation
- UK GDPR Article 9(2)(g) - reasons of substantial public interest

- DPA 2018, Sch 1, Part 2, 18 – safeguarding of children and individuals at risk; (Protection of Vulnerable Groups (Scotland) Act 2007)

11. Retention and Erasure

The College retains the data defined in this policy for the minimum periods of time required to meet its statutory duties. The Data Retention Schedules can be found on the College intranet.

12. Policy Management

This policy will be reviewed periodically, and will be made available to the ICO, upon request and without charge. It will be held and reviewed until a period of at least 6 months after the College has ceased processing such data.

13. Related Policies and Procedures

- Data Breach Procedure
- Records Management Policy
- GDPR Guides
- Equality Impact Assessment

Policy & Procedure	Business Continuity
Policy Area	Finance and Estates
Version Number	05
Approving Committee	Audit and Risk Committee
Date of Approval	24 February 2026
Date of Equality Impact Assessment	TBC
Date of Next Review	01 April 2027
Responsible Senior Manager	Director of Finance and Estates

Policy Statement

To meet the College's objectives and ensure continuity of its operations and plan for the recovery / renewal of services in the event of serious disruption.

Associated Policies/Procedures

Where applicable Procedures associated with observing the policy are contained within this policy document, listed below and available on the below link on the Staff Intranet. Template documents associated with this policy are also located in the Forms section of the Staff Intranet.

https://intranet.westcollegescotland.ac.uk/reference/SitePages/Policies%20and%20Procedures.aspx

Equality Statement

The College is committed to providing equal opportunities to ensure its students, staff, customers and visitors are treated equally regardless of gender reassignment, race, religion or belief; disability; age; marriage and civil partnerships; pregnancy and maternity; sexual orientation; sex.

Please note this document is available in other formats, to request another format please email info@wcs.ac.uk

History of Amendments

Date	Version/Pages/Sections Affected	Summary of changes
06/02/2018	Version 1	
06/05/2021	Version 2	
08/12/2021	Version 3	New policy template
March 24	Version 4	Review by VP Operations
February 26	Version 5	Review by Director of Finance

Contents

1. Scope

This document applies to all services within all the West College Scotland (the College) sites. Each faculty/department will formulate their own Business Continuity Plan (BCP), considering this document and associated guidance. Subject to approval by the appropriate Senior Leadership Team (SLT) Each faculty/department may exclude parts of their operations that they consider falling outside of the scope of their BCP's, provided that, such exclusions are documented and do not negatively impact on the College's ability to deliver its services.

This Policy does not seek to replace or supersede existing relevant policies or planning (e.g., site specific) documents. Instead, it advocates the use of existing risk registers and appropriate incident reporting mechanisms and will link closely with the College's emergency preparedness activities.

2. Introduction

The aim of having a Business Continuity Management System (BCMS) is to ensure that the College can maintain its activities in the face of disruptive challenges. Therefore, all faculties/departments are expected to prepare, exercise, maintain and review BCP's based on the principle that each faculty/department should be able to maintain its own critical activities which are key to contributing to the strategic intention of the College.

This Policy defines a broad framework for the implementation of the College's BCMS to minimise the impact of business disruption. Full compliance with this Policy will ensure procedures exist for recording, assessing, and managing business continuity risk; identifying and prioritising essential activities; responding to business disruptions or incidents, regardless of cause and maintaining essential services or restoring services to a minimum acceptable level.

3. Principles

The College's business continuity planning is devised to deal with the impact(s) of an event/situation/disruption as opposed to addressing the potential causes and such business continuity arrangements are crucial to the successful management of the College.

The strategic responsibilities for BC rest with the Vice Principal Operations and are governed by the SLT, however, viability of the College's BCMS is determined by the commitment and ownership demonstrated by the various services.

The College's SLT, through the Director of Finance and Estates (DFE) will ensure that BCPs are reviews at least annually, or earlier if subject to significant change and that any new system or activity has documented BC procedures that augment wider faculty / department planning.

The College, through the Vice Principal Operations / DFE, will provide adequate training as well as testing and exercising to validate its plans at regular intervals to ensure awareness of the requirements of this Policy.

On completion of BCPs, they should be stored securely with both an electronic and hard copy available locally as well as utilising existing software within the business continuity portal of the College Intranet and properly version controlled by the DFE.

BC planning is a dynamic, iterative, composite process, which allows for further development and adaptation as circumstances change or risks evolve.

4. Strategic BCM Aim

To develop, implement and manage a robust and effective BCMS to protect College operations, including its staff, students, visitors, and contractors were reasonably practicable.

5. Strategic BCM Objectives

The College's strategic business continuity objectives are to:

- Provide a framework for the development, implementation and monitoring of a Business Continuity Management System (BCMS)
- Identify, assess and minimise business continuity risk
- Ensure that the BCMS adequately addresses planning, processes, training and continuous improvement to manage disruptions that may affect the College or its interests
- Support the delivery of the College Corporate Plan
- Safeguard the College's reputational integrity
- Raise awareness of Business Continuity and the interdependencies between teaching and support services

6. Statement of Intent

The College is committed to developing, implementing and managing a robust and effective BCMS as a key mechanism to:

- Ensure that a formal, consistent, co-ordinated and cost-effective approach to the continuity of its teaching and support activities within the education environment
- Identify the critical activities of its business via robust Business Impact Analysis (BIA) and risk assessment
- Protect, maintain and recover business critical activities as recognised in relevant BIA

- Develop BC plans to ensure continuity of activities at a minimum acceptable level and within specified timeframes
- Develop a culture of Business Continuity Management that feeds into the College's planning and management processes
- Maintain the confidence of staff, students, other key stakeholders and visitors
- Protect and uphold the reputation of the College and manage an up to date and relevant BCMS

The SLT, through the leadership of the Vice Principal Operations, will endorse and drive the development of a strong BC culture, which is an essential ingredient to providing an effective BCMS.

The College, through the Vice Principal Operations / DFE, will implement a programme of training, exercises, maintenance and review, which will be delivered through an annual work plan.

Vice Principals, Assistant Principals and Directors will ensure that nominated Business Continuity Coordinators maintain BC plans (based on a standard template) for critical activities within their areas of responsibility.

The coordinators will maintain and review BC Plans including the Business Impact Analyses on an annual basis or sooner if significant change is required due to circumstances.

All staff who are expected to respond to a disruption, working for and on behalf of the College, must be aware of the BCP appropriate for their areas of business and their role in preparation for an event/disruption.

7. Roles and Responsibilities

This section outlines the roles and responsibilities for relevant staff in respect of BCM.

Principal

The Principal has overall responsibility for Business Continuity Management within the College however delegates this Strategic responsibility to the Vice Principal Operations to ensure implementation of this Policy throughout the College estate.

Senior Leadership Team (SLT)

The Senior Leadership Team (SLT) will:

- Ensure appropriate structures are in place to implement effective Business Continuity arrangements
- Monitor the implementation of this Policy
- Raise issues of resource necessary for the adequate control of severe BC risks at the appropriate budgetary forums.

Vice Principal Operations / Director of Finance and Estates

The Vice Principal Operations / Director of Finance and Estates have tactical and operational responsibility to implement the requirements of this Policy and ensure that:

- The SLT is provided with reasonable assurance or is kept informed of any significant business continuity risks and any associated significant developments, concerns or issues
- There is specialist advice on business continuity matters and that this is available to relevant College staff
- There is appropriate documentation identifying the Policy and guidance
- Financial support is available if BC arrangements are invoked in conjunction with the Head of Finance

- Facilitate provision of specialist advice and guidance on BCM issues including the coordination, development, implementation and review of BC plans, processes and procedures
- Provide accessible reference data by way of the College intranet
- Meet with identified faculty/department representatives to establish routine and structure, as well as the review of business impact analysis and plans on an annual basis when necessary
- Work in partnership with Head of Campus Operations were necessary to risk assess current and future threats identified through horizon scanning and intelligence gathering
- Coordinating annual update of departmental BC plans
- Embed a Business Continuity culture through communication and the provision of awareness sessions, training and exercises to staff, according to their roles and needs
- Facilitate training, tests and exercise
- Audit compliance of BC plans
- Provide recommendations and other management feedback as appropriate
- Represent the College in the wider education business continuity arena

Local Continuity Management Teams

As part of the planning and response arrangements for any incident, which invokes the BC plans, critical business steam representatives and coordinators roles will be nominated by the SLT.

Having taken part in the preparation of Business Impact Analysis. These individuals will form the teams which will enact the BC response when an incident occurs. They will also conduct the annual review of arrangements pertinent to their area.

(IMT)

Upon the occurrence of a disruptive event, involving wider consequences across the College estate, it may be necessary to escalate the response. The College IMT, whose representatives are pre-determined from across the College services, will convene to provide leadership, coordination, communication and decision making during multi-agency coordination of emergency response.

A nominated individual will be identified by the Leader of the IMT to represent the College during multi-agency coordination of emergency response.

8. Incident Reporting and Debriefing

Business continuity incidents should be reported if the appropriate criteria is met (criteria for reporting is contained within the associated guidance manual) and debriefs should be coordinated by the leader of the IMT to ensure that learning and review informs continuous improvement.

9. Insurance

As part of the Risk Assessment, development, implementation and review of business continuity plans any decision to treat, tolerate, terminate or transfer risk for indemnification purposes must be documented and appropriate consultation sought with the Director of Finance and Estates.

10. Procurement

The College has a number of suppliers and partners upon whom it relies on to provide a continued service. In order to minimise any risk of disruption, by failure to supply a product or service, suppliers and partners identified as critical in the relevant Business Impact Analysis will be requested to provide assurances that they have BC arrangements in place.

Those responsible for commissioning or procuring goods or services from external suppliers should consult the Procurement Manager to ensure contracts and/or service level agreements contain the appropriate clauses in respect of business continuity.

11. Governance

The Senior Leadership Team (SLT) will convene annually to oversee the implementation and monitoring of the College's BCM Policy. This group will be chaired by the Vice Principal Operations and will be supplemented by staff from cross-College operations as required.

The organisation has set out clear Recovery Point Objectives (RPOs) so everyone understands how much data loss is acceptable in the event of a disruption, see also operational plans. This helps teams prioritise what systems need the most frequent backups and ensures that recovery expectations are realistic and agreed.

12. Training, Awareness and Exercising - Maintenance and Review

BC plans are to be validated at regular intervals to determine whether any changes are required to procedures and responsibilities. Planned review periods should not exceed 12 months.

The Vice Principal Operations / Director of Finance and Estates will:

- Develop and source a suitable programme of training in BCM and BC risk management
- Identify appropriate levels of training and awareness for staff, to enable

cascade through their areas of activity to affect a strong BC culture across the College

- Organise exercises of the BC plans and advise on local exercising arrangements
- Prepare and monitor the annual resilience work/action plan

13. Cyber / Terrorist Attack / Martyn's Law

A cyber-attack or terrorist threat poses a significant risk to the continuity of College operations, potentially disrupting critical systems, compromising sensitive data, and impacting the safety of staff, students, and visitors. In the event of such an incident, the College will activate its incident response and communication protocols, isolate affected systems or areas, and work with relevant authorities to assess the threat, contain the impact, and restore essential services. Maintaining robust cybersecurity measures, physical security controls, and clear escalation procedures is essential to ensuring the College can respond quickly, protect its community, and resume normal operations as safely and efficiently as possible.

IT already maintains a separate disaster recovery and backup plan, which outlines the technical processes for restoring systems and data. The technical detail remains within IT's own plan.

Martyn's Law (the Terrorism (Protection of Premises) Bill) introduces a strengthened duty for organisations to enhance public safety by improving preparedness for, and resilience to, potential terrorist incidents. In line with this legislation, the College will ensure proportionate security measures are in place across all campuses, including risk assessments, staff awareness, incident response planning, and clear evacuation and lockdown procedures. Compliance with Martyn's Law supports the College's wider business continuity arrangements by ensuring that staff and students are better protected, that emergency actions can be taken swiftly and effectively, and that the organisation is equipped to respond to and recover from a terrorism-related incident with minimal disruption to critical operations.

14. Monitoring

The organisation will carry out a simulation exercise to test how well the BCP works in

real conditions. A planned exercise allows teams to walk through the steps, identify gaps, and make improvements before a real incident occurs.

This Policy will be reviewed annually. The College will commission additional work or change the monitoring arrangements to meet the organisational needs.

15. Appendix A – Definitions

Business Continuity Management System (BCMS)

An ongoing Management and Governance process supported by the College Senior Leadership Team (SLT) and appropriately resourced to implement and maintain Business Continuity Management.

Business Continuity Management (BCM)

The holistic management process that identifies potential threats to the College and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its Colleges and services, reputation and value creating activities.

Business Continuity (BC)

The capability for the College to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level.

Business Continuity Incident (BCI)

An event or occurrence that disrupts an organisation's ability to deliver normal service and where contingency arrangements are required to return them to an acceptable level.

Business Continuity Plan (BCP)

A clearly defined, documents and predetermined plan for use when business operations are disrupted by an event. Typically, the plan covers loss of premises, information, people, stock or other technologies.

Business Impact Analysis (BIA)

The process of analysing business activities which support wider organisational products and services, determining threats and risks and the effect business disruption may have on organisational viability.

Risk

Identification of potential vulnerability-based likelihood and impact.

Risk Assessment (RA)

The overall process of risk identification, analysis and evaluation.

Maximum Tolerable Period of Disruption (MTPD)

The point at which an organisations viability will be irrevocably threatened if the critical activities cannot be resumed.

Recovery Time Objective (RTO)

The target time for the resumption of a critical activity after an event.

Business Continuity Plan

Version: V9

Date: February 2025

Owner: Vice Principal Operations

VERSION CONTROL

Version	Modified on	Modified by	Details
6	31 July 2022	Alan Ritchie Jill McDonald	Plan updated – annual review and contact details updated
7	31 January 2023	Alan Ritchie Jill McDonald	Updates following management changes and exercise suggestions
8	30 January 2024	Julie McLaughlin	Update Job Role Titles
9	10 February 2025	Mark Doyle	Review and update following management review and recommendations

Updated versions of Business Continuity Plan will be issued on the Teams site and a note sent out to all Team members that an updated version is available.

1. Introduction

The purpose of the Business Continuity Plan (BCP) is to assist the College to prepare and respond to incidents that could cause significant disruptions to normal activities. To keep the BCP up to date and relevant, it will be reviewed annually or following any critical incident; any significant changes to the hardware and critical systems covered in the BCP; or following any significant changes to our organisational structure or processes. When changes are made an updated version of BCP will be made available on the Teams site and a notification sent to all members of the Team. Access to the Teams site will be limited to those members of staff who require to access the information on the site, and it will not be publicly available.

The BCP will be held securely as follows:

- An online copy in the Business Continuity Teams site
- A printed copy will be held in the Battle Boxes at each of our four main sites, being Clydebank, Greenock Finnart Street, Greenock Waterfront and Paisley. Battle Boxes are held in the Senior Leadership offices at Clydebank, Greenock and Paisley and at Reception at Waterfront Campus.

The BCP will include an up-to-date contact list for key stakeholders or organisations that may be involved in any incidents. Which includes staff, internal and external stakeholders, suppliers, and emergency services will also be included within the Teams site (see Business Continuity Contact sheet).

The BCP is the main reference document for use following a major incident. It sets out the generic response to any incident. In addition to this BCP, further BCPs will be developed to address specific scenarios defined during the risk analysis stage.

2. Scope

The BCP sets out how the College will respond to incidents causing significant disruptions to normal operations. The BCP is not supposed to cover every possible disruption. It is written to establish clear roles and responsibilities that will allow the management of the College to respond quickly and effectively to significant disruptions. The BCP applies to incidents happening at any College site. It may also have to be used following incidents off site that involve College students or staff.

The BCP is not intended to cover day to day operational disruptions that managers deal with regularly. It is to be used when there could be significant effect on operations, students, staff,

the environment and the reputation of the College, but to address potential risks identified during the risk analysis stage.

3. Definition of an Incident

Incidents are events that have the potential to cause significant disruption to normal operations. The following list is not exhaustive, however there is an expectation a member of the Incident Management Team (IMT) would be notified and then decide if the BCP should be invoked:

- Any incident that would cause a closure of any College site for one working day or more e.g. extreme weather, fire, flood or loss of utilities or too few staff available to continue operations
- Loss of access or damage to a critical room within a building likely to cause one day or more disruption to business as usual. Critical rooms could include catering facilities, Plant room, data centres or specialist teaching facilities
- Any incident that has or could result in a reportable incident under RIDDOR (Reporting of Injuries, Diseases, and Dangerous Occurrences Regulations) or that could trigger a Health & Safety Executive investigation
- Any violent incident, or threat of violence, involving staff or students
- Any threat (terrorist or otherwise) made against the College. Martyn's Law (Protect Duty) requirements ensure proportionate security measures, threat awareness, and preparedness arrangements are embedded within the College's incident response and continuity planning. This is captured in the BCP policy.
- Any incident that requires emergency services to be called to a College site
- Any violent incident involving a member of the public, contractor or visitor on a College site
- Any incident that could have a significant reputational impact, e.g. a negative story in a local paper

4. Activation of BCP - Who to contact

A manager may become aware of a potential incident which has a possibility of becoming a material or significant incident. In such a case the manager should inform a member of the Senior Leadership Team (SLT) as soon as possible. An outline of the incident should be provided and that the manager will continue to investigate the matter and report back to the SLT member. If possible, a timescale should be established to ensure that the matter is not discarded. This is a precautionary stage which will allow the SLT member to put on notice the IMT members that they may be required. This precautionary stage should be conducted by phone rather than email

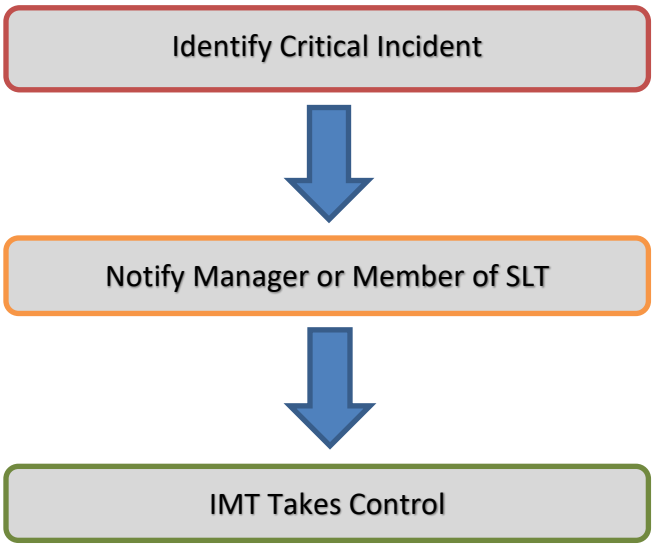
to ensure that the message has been received. Instant messaging can be used if unable to make contact by phone and only by email as a last resort.

As soon as a critical incident has been identified, the member of staff must notify their line manager. The line manager will contact a member of the Senior Leadership Team (SLT). If the line manager is not available, then contact the nearest manager or a member of the SLT.

For contact details of all relevant staff / stakeholders please see Teams site – Business Continuity Contact Details.

The College maintains a WhatsApp Business Continuity Group which allows IMT members to be informed immediately about a pending or actual incident. The members of this WhatsApp Group will be reviewed at least annually in line with the requirement to review the overall Business Continuity Plan. The use of WhatsApp should be limited to general information and not specific data / critical information. Where specific information needs to be shared the Business Continuity Teams site should be used for this purpose.

Once notified of a critical incident, the SLT / Manager will pull together the Incident Management Team (IMT) led by the Vice Principal of Operations (VPO) who will assume lead responsibility. Where the VPO is unavailable when an incident takes place, another member of the SLT will assume the authority to make any decisions required. Staff will be co-opted onto the team depending on the nature of the incident.



The decision to activate this Plan will normally be made by a member of the College Executive. Any decision to close a campus following an incident must also be made by the Executive. Should a member of the Executive not be available then the decision to activate BCP can be initiated by:

- Director of Finance and Estates
- Any Member of SLT
- Senior Presence (SLT / Head)

The member of staff who is activating the BCP should take charge of ensuring that all members of the IMT are contacted. The information to be conveyed to the members should include:

- Reason for the phone call
- Time, location, and nature of the incident
- What action is required next

Outside of core hours the Estates Call-Out Procedure will be followed until a member of the IMT is alerted to the incident. If the incident can be dealt with by the Estates staff it will be closed off. However, should this not be the case, the Estates staff will make contact with the relevant member of staff and BCP will be activated as required.

5. Incident Management Hierarchy

Incident Management Team (IMT)

The IMT is responsible for incidents. The primary role of the team is:

- To assess the situation by gathering information from as many sources as possible
- Agree an Action Plan to protect human life, the environment, the College's assets and the reputation of the College
- Communicate with key (internal & external) stakeholders throughout, including both teaching and support staff unions
- Review progress throughout any disruption and take appropriate decisions to get back to normal operations
- Ensure lessons are learned following any incidents to prevent future losses or be better prepared to cope if they do happen.

The IMT is made up of 'core' and 'non-core' team members.

Core Team Members:

- Vice Principal of Operations (IMT Leader)
- Vice Principal of Educational Leadership
- Director of IT and Digital Transformation
- Director of Finance and Estates
- Director of Organisational Development and HR
- Director of Student Experience
- Head of Campus Operations
- PA to Executives
- PA to SLT

Non-Core Team Members:

- Health and Safety Advisors
- Estates Managers
- Heads of Sector / Department

It is expected all members of the core team (or their deputies) will be involved in the response to most incidents. Non-core team members may be asked to join the team depending on the circumstances, for example if specialist operational or technical advice is needed. All team members have a nominated deputy. Some deputies will be asked to join the IMT while others may be consulted or asked to provide technical or operational advice in the absence of the primary IMT member.

6. Command Centres

The IMT require a room to meet and manage the response to the incident from the most appropriate command centre. Each command centre should provide the following:

- Access to the College ICT networks
- Space for all members of the IMT to get around a table
- Whiteboards or flipcharts for note taking

Command centre locations are as follows, although will be subject to change in regard to the circumstances of the incident:

PAISLEY

Executive Suite Renfrew Building — Phone: 0141 581 2211
Glynhill Hotel - 169 Paisley Road, Renfrew PA4 8XB
Brian Spence (brian@glynhill.com) — Phone: 0141 886 5555

CLYDEBANK

SLT Suite 3rd floor — Phone: 0141 951 7412
Room 001 (just off reception)
Golden Jubilee Conference Hotel – Beardmore Street — Phone: 0141 951 6000
Glasgow, G81 4SA
Denis Flanagan (denis.flanagan@goldenjubilee.scot.nhs.uk)

GREENOCK

Leadership Suite 1st floor — Phone: 01475 553001
Student Services area off main reception — Phone: 01475 724433
Tontine Hotel - 6 Ardgowan Square, Greenock PA16 8NG — Phone: 01475 723316

7. Recording and Monitoring

It will be essential to keep a log of actions taken and by whom to report on what happened, what was done and the results and outcomes of a critical incident. The Critical Incident Log Sheet should be used for this purpose and should be managed by a delegated member of the IMT (See Appendix A for an example of the format to be used).

Other formats of incident logging may be more appropriate and will depend on the circumstances – use of a whiteboard (remember to take photograph of content before wiping clear), Teams tasks can be used, Outlook tasks can also be used. The aim is to ensure that a log of actions is taken, and resolutions are maintained for future reference. The incident log will be used for insurance purposes or may be required for follow up investigations.

A member of the IMT should be delegated to be the central point of contact for all enquiries. These enquiries should be recorded on an Enquiry Log (see Appendix B for an example of the format to be used). As the enquires are addressed they should be scored through but not deleted. This will allow any member of the IMT to pick up the Enquiry Log and continue to deal with enquiries in the absence of the delegated IMT member.

8. Investigation and Analysis

Following the Recording and Monitoring process, the Critical Incident Log (Appendix A) will form the basis of the investigation and analysis after any critical event, together with the Incident Assessment Checklist (see Appendix D). Any investigation should enable us to understand:

- What caused the incident
- Could the incident have been prevented
- Were there any underlying failures in health and safety management
- What lessons have been learned – is there anything we need to do differently?
- What actions are required to prevent or minimise a recurrence

One of the main benefits of investigating, analysing and reporting on an incident is to contribute to the corporate knowledge held by an organisation. It is therefore important that this information be discussed and shared with staff as deemed appropriate by the IMT.

9. Communications

Emergency Communications

In the event of an emergency, the Director of Student Experience or a Marketing & PR Executive should be contacted at the earliest opportunity to allow them to assess the scale and nature of possible media interest and to decide upon an appropriate response, if it is judged that a response is required.

The College has developed a Major Incident Communications Response Manual which can be found on the Business Continuity Teams site. The manual is designed to support the containment and subsequent recovery from a serious reputational issue. The manual provides practical guidance on how to assess an incident and what the potential response could be. It is advised that all staff involved in the business continuity process make themselves familiar with the contents of the manual in advance of any incident.

It is important that any response the College may choose to give is informed by all the available information and by a judgement as to what is in the best interests of the College's staff and students. Therefore, in no circumstances should any member of staff offer comment on behalf of the College to any media outlet without first liaising with the Communications Directorate.
For similar reasons, all media requests for comment and broadcast interviews (live or pre-recorded) must be directed to the Communications Directorate.

Should the College choose to respond to media requests it will do so in the name of the Principal or a "College Spokesperson". In the event of the Principal being unavailable, comment will be issued in the name of one of the two Vice Principals, with their prior consent. Comment will usually be issued to media outlets via email and, if practical, on the College's social media platforms.

Should the College accept requests for broadcast interviews, these will be conducted, whenever possible, by the Principal. In the event of the Principal being unavailable and depending on the emergency and the nature of the interview requested, the Vice Principals and the Director of Student Experience will decide who among themselves should conduct the interview.

Communication to Staff / Unions

Make sure regular updates are provided to staff and unions about the incident and how they should deal with it:

- Information will be disseminated from the IMT to all staff. This will be via a communication tree process, whereby the message is handed down from SLT level to Senior Manager Level and so on.
- The IMT should also consider at which point to inform the unions of the incident. It is likely that staff will directly approach their union representatives in the case of an incident. By keeping the unions informed this will assist in ensuring that any messaging is communicated effectively.
- The data in the communication tree must be revised following any changes to staffing and must be accessible to all staff taking responsibility for passing on the communication.
- The primary information channel used to communicate will depend on the issue being experienced.
- Some communication may be required across the organisational structure. All members of SLT should therefore hold each other's emergency contact details.
- The IMT will decide who should know what about the incident and when they should know about the incident.
- The IMT will specify to staff what message is to go out to external stakeholders.
- All enquiries coming in and out from the main contact phoneline / email address should be recorded on an Enquiry Log (see Appendix B)

10. Closure Protocol

Decision to close any campus or the whole College must be taken by Principal and/or VP and only in exceptional circumstances will the decision to close be taken by member of SLT.

If decision to close a main campus is taken, consideration should be given to whether the closure of local satellite sites is also merited i.e. if a weather-related incident occurs.

Decision will be taken on advice of:

- Local Authorities who will potentially close schools and other local services

- West Dunbartonshire
  https://twitter.com/WDCouncil

  https://www.west-dunbarton.gov.uk/emergencies/severe-weather/school-and-nursery-closures/

- Renfrewshire
  RenCouncil (@RenCouncil) / Twitter

  https://www.renfrewshire.gov.uk/

- Inverclyde
  Inverclyde Council (@inverclyde) / Twitter

  http://www.inverclyde.gov.uk/advice-and-benefits/winter/

- Ready Scotland
  https://twitter.com/readyscotland

  http://readyscotland.org/

- Advice from Met Office
  http://www.metoffice.gov.uk/public/weather/warnings/#?tab=warnings&map=Warnings&zoom=5&lon=-3.50&lat=55.50&fcTime=1422403200

- Local staff who are present at the campus

Based on review of the above information by the IMT Leader, the decision to close will be taken by Principal / VP as early as possible.

In terms of communicating closure, the following will be initiated by stated staff member or by deputy. Communication to all staff to include as a minimum whole / partial closure, reason for the closure, anticipated length of the closure, to refer to website and social media for updates:

- Communication to Principal – IMT Leader
- Communication to VP – IMT Leader
- Communication to AP / Director – VP with direct line management responsibility
- Communication to immediate managers to inform them of closure – AP / Director
- Communicated to Estates Staff / H&S Managers – Director of Finance and Estates
- College telephone outgoing message to be updated – Director of IT and Digital Transformation
- Student and Staff College email – IMT Leader
- Website, College Intranet, Facebook and Twitter – Director of Student Experience
- Message on MyDay platform - Director of Student Experience
- Text message to students and staff – Director of Student Experience
- Media if necessary - Director of Student Experience

11. Loss of Premises

In the event of loss of one or more of our premises, where possible activity should be moved to other campuses, if this is not possible then external stakeholders must be contacted to arrange alternative temporary accommodation. For main departmental contact details refer to individual departmental Business Continuity Plans which are available on the Teams site.

12. Loss of IT

Please refer to the Vice Principal Operations for the Cyber Incident Response Plan (CIRP) and IT Disaster Recovery Plan (DRP) to be implemented. The CIRP is held on the Business Continuity Teams site and is available to permitted staff.

13. In the Event of a Fire

Should a fire break out follow the Business Continuity Plan for a Fire (see Appendix E).

14. Terror Attack

In the event of a terrorist attack affecting the College, the Business Continuity Plan will be activated immediately to safeguard life, support emergency services, and maintain critical operations. The Incident Management Team will coordinate the response, ensuring rapid evacuation or lockdown as directed by Police Scotland, clear communication to staff and students, and swift implementation of alternative arrangements for essential services. Post-incident actions will focus on welfare support, stabilising operations, restoring priority functions, and working with authorities during investigation and recovery phases to ensure a safe and structured return to normal activity.

15. Other Issues including Staffing

Outbreak of disease (e.g., influenza pandemic)

- An influenza pandemic or similar occurrence may jeopardise staffing levels, directly though staff illness, or indirectly through fear of infection or through caring responsibilities for sick relatives. It is essential information is disseminated about how to identify symptoms of flu and what to do in the event of a member of staff becoming ill with suspected flu.
- In the event of a pandemic, any staff infected by the virus must remain off work to minimise spread. Staff who display symptoms should be sent home and advised not to return to work until they have fully recovered.
- IMT should identify the key functions of the College that must continue and establish if there are any departments with key person dependencies.
- From the business impact assessments, the IMT will be able to identify at what stage the staffing level is considered to be critical and how this differs departmentally/per key function depending on the time of year. This is particularly relevant for smaller departments where very few staff absences could mean the loss of a function.
- It must be recognised that it may be necessary to limit annual leave in order to sustain services.
- The IMT should prioritise keeping critical systems operating so that our online facilities continue to function for our stakeholders.

Fuel Shortage

In the event of a widespread fuel shortage, options will include:

- Increased use of public transport
- Car sharing
- Walking or cycling

When information indicates that a fuel shortage is expected, a list of staff living remotely from their place of work and with difficulties in accessing any of the above options will be compiled.

Industrial Action

As far as possible, without attempting to influence staff members' legal right to take industrial action, managers should try to estimate the proportion of staff that may be available to work in order to plan work in accordance with priorities.

Severe Weather

The College takes the safety of its employees very seriously and would not expect anyone to make the journey into work if this is likely to put then in any danger. Employees are however required to consider any reasonable alternatives to their normal method of transport (e.g., taking a train or bus instead of a private car) before making the decision not to come in. See also Hybrid Working Policy.

In the event that weather conditions deteriorate during the working day, and it appears that employees could have difficulty in travelling home the Principal or any other member of the Executive may decide to close the campus / College early to ensure employees are able to get home safely. The term of Severe Weather Employer Guidance would apply.

Appendix A – Critical Incident Log Sheet

Date	Time	Critical Incident description	Action Taken and by whom	Outcome	Incident closure time

Appendix B –Enquiry Log

Date	Time	Name of person making the enquiry	Organisation represented	Contact number / email address	Notes on enquiry	Action required	Status (Resolved / Unresolved)

Appendix C – Plan Test / Exercise Log

Date of test	Nature / description of exercise	Person responsible	Other personnel involved	Learning points of exercise	Action required (including date and person responsible)

Appendix D – Incident Assessment Checklist

The checklist is designed to be used following a major incident. Not all information will be known in the early stages. The checklist should therefor prompt the IMT to revisit what is known and what needs further investigation throughout the incident.

Questions	Response
What is known about the Incident? Emergency services alerted? Has the site evacuated fully? Type of incident, e.g., fire, ICT failure etc. No. of injuries and deaths confirmed Who reported it, when and how?	
Is there likely to be any external organisations involved? Emergency Services HSE	
Have lines of communication been opened with them? Please note name & number of the contact	
What is the impact (or anticipated impact) on normal operations? Sites or buildings affected? Consider satellite buildings in any decision process	

Questions	Response
3rd parties who use College facilities or are adjacent to College sites? Are there any special events taking place or coming up? Is this likely to disrupt a full day of 'normal' operations?	
Do you have any concerns about staff or student welfare resulting from the incident?	
Has the IMT been notified? Do all team members need to be involved? Are there any team members unavailable?	
Is there likely to be media interest in the incident? If so ensure that the following are informed: Director of Student Experience Principal Chair of the Board of Management	
What are functional departments doing about the incident? Support departments: Estates	

Questions	Response
IT Catering Student Support/Funding Marketing / Communications HR MIS Finance	
Consider invoking the Incident Management Plan.	

Appendix E – Business Continuity Plan for a Fire

No	Actions	Notes	Priority / Timing	Accountability	Complete ✓
1	Initiate Fire Evacuation Plan		High	IMT Leader	
2	Hand over site to fire brigade		High	H&S Advisors / Senior Presence	
3	Convene IMT at appropriate command centre location		High	IMT Leader	
.4	Activate Incident Management Plan		High	IMT Leader	
5	Contact Executive to advise		High	IMT Leader	
6	Assign staff member to consult with Fire Brigade		High	IMT Leader	
7	Make assessment of likely duration of Incidents and impact on operation		High	IMT Leader	
8	Decide if staff and occupiers should remain on site or be sent home		High	IMT Leader	
9	Identify key internal stakeholders		High	IMT Leader	
10	Draft communication to staff		High	Marketing	

Audit & Risk Committee

Wednesday 11 March 2026

Agenda Item: 08

Title of Paper	Annual review of the effectiveness of the Audit & Risk Committee and Internal Auditors.
Presented by:	Susan McDonald, Governance Manager
Status	PUBLIC
Recommendation:	**For Approval**
Linked To:	
KPI(s)	**n/a**
Strategic Objective	**n/a**
Strategic Risk	**Governance Compliance & Reputational**

Purpose / Executive Summary:

This report outlines the process which it is proposed the Audit & Risk Committee adopts for the 2025-26 review of its effectiveness and that of the internal auditors. The procedure follows that agreed in previous years which is to issue two questionnaires covering:

- Audit & Risk Committee Effectiveness.
- Evaluation of the Internal Auditors.

It is intended the questionnaires will be issued following the Audit & Risk Committee meeting held on 11 March 2026, with a report on the outcome submitted to the 27 May 2026 Committee.

The purpose of this report is to consider and agree the approach to be taken and the timetable for this work.

The paper is presented in line with the following West College Scotland Audit & Risk Committee Terms of Reference:

- *"To review its own effectiveness at least annually and to report the results of that review to the Board."*
- *"To review the scope, efficiency and effectiveness of the work of the Internal Auditors and to advise the Board on these matters."*

Recommendations:

The Audit & Risk Committee is asked to consider **and approve** the suggested process which includes:

a) the distribution list to be used to evaluate the effectiveness of the Audit & Risk Committee and of the Internal Audit function.

b) Both questionnaires to be used for the evaluation.

Implications:	
Financial	There are no direct financial implications in this report
Student Experience	There are no direct student experience implications associated with this report
People	There are no people implications associated with this report
Legal	There are no direct legal implications in this report
Reputational	There are no financial implications in this report
Community/ Partnership impact	There are no community or partnership implications in this report
Environment	There are no environmental implications in this report
Equalities	There are no equality implications in this report

Background

External Audit Review

A summary on the evaluation of the External Auditor immediately following the completion of the external audit work will be submitted to the March Audit & Risk Committee Meeting. At the time of writing, we still await information from Audit Scotland on the review of the External Auditor's performance.

Audit & Risk Committee Effectiveness

The effectiveness review of the committee will take place during late March / April 2026.

It is proposed to use the same questionnaire as used previously, a copy of which has been included for agreement. The questionnaire used to evaluate the effectiveness of the Audit & Risk Committee is based upon the requirements of the Scottish Government Audit and Assurance Committee Handbook, supplemented by further good practice questions as proposed by the National Audit Office.

As per previous years, and in line with good practice, it is the intention to issue the questionnaire to members of the committee and other regular attendees.

Internal Audit Review

The proposed questionnaire used to evaluate the internal audit function is as used for last year's evaluation. This was updated based on a best practice guide issued by KPMG and complies with the requirements of the Scottish Government Audit and Assurance Committee Handbook.

Next Steps

If the Committee is satisfied with the proposed approach, the questionnaires will be issued following this Committee meeting and by no later than Thursday 26 March 2026.

Members will be asked to return the completed questionnaires to the Governance Manager by no later than Friday 24 April 2026, who will provide an anonymised analysis of the response to the 27 May 2026 committee meeting and the June Board.

The questionnaire will be issued to:

- All Audit & Risk Committee members, including Co-opted Members.
- Principal.
- Vice Principals.
- Director of Finance & Estates

A report on the outcome of the surveys will be provided to the 27 May 26 Audit & Risk Committee meeting for consideration and action as appropriate. Thereafter, the Audit & Risk Committee will report to the June 2026 Board of Management on its findings along with other Committee and Board self-evaluation reviews.

Recommendations:

The Audit & Risk Committee is asked to consider **and approve** the suggested process which includes:

a) the distribution list to be used to evaluate the effectiveness of the Audit & Risk Committee and of the Internal Audit function.
b) The same questionnaires to be used, as was used for last year's evaluation.
c) The timeline for responses.

AUDIT COMMITTEE SELF-ASSESSMENT CHECKLIST

	YES/NO/NA Don't know	Comments/Action
Role and Remit		
Does the audit committee have written terms of reference?		
Do the terms of reference cover the core functions of an audit committee as identified in the *SG Audit and Assurance Committee Handbook*?		
Are the terms of reference approved by the audit committee and reviewed periodically?		
Has the audit committee been provided with sufficient membership, authority and resources to perform its role effectively and independently?		
Does the body's governance statement mention the audit committee's establishment and its broad purpose?		
Does the audit committee periodically assess its own effectiveness?		
Membership, induction and training	**YES/NO/NA Don't know**	**Comments/Action**
Has the membership of the audit committee been formally agreed by the management board and or Accountable Officer and a quorum set?		
Are members appointed for a fixed term?		
Does at least one of the audit committee members have a financial background?		
Are all members, including the chair, independent of the executive function?		
Are new audit committee members provided with an appropriate induction?		
Has each member formally declared his or her business interests?		
Are members sufficiently independent of the other key committees of the Board?		
Has the audit committee considered the arrangements for assessing the attendance and performance of each member?		
Meetings	**YES/NO/NA Don't know**	**Comments/Action**
Does the audit committee meet regularly, at least four times a year?		
Do the terms of reference set out the frequency and broad timing of meetings?		

Does the audit committee calendar meet the body's business and governance needs, as well as the requirements of the financial reporting calendar?		
Are members attending meetings on a regular basis and if not, is appropriate action taken?		
Does the Accountable Officer attend all meetings and, if not, is he/she provided with a record of discussions?		
Does the audit committee have the benefit of attendance of appropriate officials at its meetings, including representatives from internal audit, external audit and finance?		
Internal control	**YES/NO/NA Don't know**	**Comments/Action**
Does the audit committee consider the findings of annual reviews by internal audit and others, on the effectiveness of the arrangements for risk management, control and governance?		
Does the audit committee consider the findings of reviews on the effectiveness of the system of internal control?		
Does the audit committee have responsibility for review of the draft governance statement and does it consider it separately from the accounts?		
Does the audit committee consider how accurate and meaningful the governance statement is?		
Does the audit committee satisfy itself that the arrangements for risk management, control and governance have operated effectively throughout the reporting period?		
Has the audit committee considered how it should coordinate with other committees that may have responsibility for risk management and corporate governance?		
Has the audit committee satisfied itself that the body has adopted appropriate arrangements to counter and deal with fraud?		
Has the audit committee been made aware of the role of risk management in the preparation of the internal audit plan?		
Does the audit committee's terms of reference include oversight of the risk management process?		
Does the audit committee consider assurances provided by senior staff?		

Does the audit committee receive and consider stewardship reports from senior staff in the key business areas such as Finance, HR, ICT?		
Financial reporting and regulatory matters	**YES/NO/NA Don't know**	**Comments/Action**
Is the audit committee's role in the consideration of the annual accounts clearly defined?		
Does the audit committee consider, as appropriate:		
• the suitability of accounting policies and treatments		
• major judgements made		
• large write-offs		
• changes in accounting treatment		
• the reasonableness of accounting estimates		
• the narrative aspects of reporting?		
Is an audit committee meeting scheduled to receive the external auditor's report to those charged with governance including a discussion of proposed adjustments to the accounts and other issues arising from the audit?		
Does the audit committee review management's letter of representation?		
Does the audit committee gain an understanding of management's procedures for preparing the body's annual accounts?		
Does the audit committee have a mechanism to keep it aware of topical legal and regulatory issues?		
Internal Audit	**YES/NO/NA Don't know**	**Comments/Action**
Does the Head of Internal Audit attend meetings of the audit committee?		
Does the audit committee approve, annually and in detail, the internal audit plans including consideration of whether the scope of internal audit work addresses the body's significant risks?		
Does internal audit have a direct reporting line, if required, to the audit committee?		
As well as an annual report from the Head of Internal Audit, does the audit committee receive progress reports from the internal audit service?		

Are outputs from follow-up audits by internal audit monitored by the audit committee and does the committee consider the adequacy of implementation of recommendations?		
If considered necessary, is the audit committee chair able to hold private discussions with the Head of Internal Audit?		
Is there appropriate co-operation between the internal and external auditors?		
Does the audit committee review the adequacy of internal audit staffing and other resources?		
Are internal audit performance measures monitored by the audit committee?		
Has the audit committee considered the information it wishes to receive from internal audit?		
Do formal terms of reference exist defining internal audit's objectives, responsibilities, authority and reporting lines?		
External Audit	**YES/NO/NA Don't know**	**Comments/Action**
Does the external audit representative attend meetings of the audit committee?		
Do the external auditors present and discuss their audit plans and strategy with the audit committee (recognising the statutory duties of external audit)?		
Does the audit committee chair hold periodic private discussions with the external auditor?		
Does the audit committee review the external auditor's annual report to those charged with governance?		
Does the audit committee ensure that officials are monitoring action taken to implement external audit recommendations?		
Are reports on the work of external audit presented to the audit committee?		
Does the audit committee assess the performance of external audit?		
Does the audit committee consider the external audit fee?		The fee is set by Audit Scotland
Administration	**YES/NO/NA Don't know**	**Comments/Action**
Does the audit committee have a designated secretariat?		

Are agenda papers circulated in advance of meetings to allow adequate preparation by audit committee members?		
Do reports to the audit committee communicate relevant information at the right frequency, time, and in a format that is effective?		
Does the audit committee issue guidelines and/or a pro forma concerning the format and content of the papers to be presented?		
Are minutes prepared and circulated promptly to the appropriate people, including all members of the Board?		
Is a report on matters arising presented or does the chair raise them at the audit committee's next meeting?		
Do action points indicate who is to perform what and by when?		
Does the audit committee provide an effective annual report on its own activities?		
Overall	**YES/NO/NA Don't know**	**Comments/Action**
Does the audit committee effectively contribute to the overall control environment of the organisation?		
Are there any areas where the audit committee could improve upon its current level of effectiveness?		
Does the audit committee seek feedback on its performance from the Board and Accountable Officer?		

Extracted from the Scottish Government Audit and Assurance Committee Handbook 2023

Evaluation of the Internal Auditors	Yes	No	Not sure	Comments
Questions for Audit & Risk Committee Members				
1. Did the auditors meet with the Audit & Risk Committee when requested?				
2. Did the auditors adequately assess controls in place within the College?				
3. Did the auditors inform the Audit & Risk Committee of any risks of which the Committee was not previously aware?				
4. Did the auditors communicate issues freely with the Audit & Risk Committee, or did they seem protective of management?				
5. Does it appear that management exercises influence on the internal auditors?				
6. Does it appear that the internal auditors are reluctant or hesitant to raise issues that would reflect negatively on management?				
7. Is the Audit & Risk Committee satisfied with the planning and conduct of the audits?				
8. Is the Audit & Risk Committee satisfied with its relationship with the internal auditors? In making this decision, the Audit & Risk Committee should consider whether: (*a*) the partner-in-charge of the audit participated in Committee meetings. (*b*) the auditors were frank and complete in the required discussions with the Committee. (*c*) the auditors were frank and complete during executive sessions with the Committee. (*d*) the auditors are on-time in their delivery of services to the College.				

Evaluation of the Internal Auditors	Yes	No	Not sure	Comments
Questions for Audit & Risk Committee Members (continued)				
9. Is the Committee satisfied that the internal auditors remain independent and objective both in fact and appearance? This response should consider: • Review all audit-related and non-audit services conducted by the internal auditors in the prior year. • Review whether the firm, the office or the partner is dependent on the College for a material percentage of its fee income. • Review whether former members of the audit team are now employed by the College. If any of these conditions exist, the Committee should consider whether they impair the auditors' independence with respect to the College.				
10. Was the audit fee fair and reasonable in relation to what the Committee knows about fees charged to other non-profit Colleges, and in line with fee benchmarking data the Committee might have available to it?				
11. Did the internal auditors provide constructive observations, implications, and recommendations in areas needing improvement?				
12. Did the internal auditors demonstrate an ongoing understanding of the uniqueness of further education?				

Signed: **Print Name:**

Date:

Based on the Scottish Government Audit and Assurance Committee Handbook 2018

Evaluation of the Internal Auditors	Yes	No	Not sure	Comments
Questions for the Principal and Chief Executive				
1. From your perspective, in working with the internal auditors are you satisfied with the scope, nature, extent, and timing of testing performed by the internal auditors?				
2. Are you satisfied with the knowledge, skills, and abilities of the staff assigned to the audit work?				
3. Are you satisfied with the engagement leadership assigned, including the partner(s), manager(s), and fieldwork leaders?				
4. Did the internal auditors provide constructive observations, implications, and recommendations in areas needing improvement?				
5. *a.* If the choice were yours, would you hire the firm to conduct next year's internal audits?				
b. If yes, are there any changes you would make?				
6. Are you satisfied with the quality and quantity of information provided by the internal auditors relative to the general progress of the audits?				
7. Were identified problems or potential issues brought to your attention in sufficient time to be addressed without delaying or extending the completion of the audits?				

Signed: **Print Name:**

Date:

Extracted from the Scottish Government Audit Committee Handbook 2008

Evaluation of the Internal Auditors	Yes	No	Not sure	Comments
Questions for the Vice Principals and Director of Finance & Estates				
1. From your perspective in working with the internal auditors, are you satisfied with the scope, nature, extent, and timing of testing performed by the internal auditors?				
2. Did the internal auditors work with you to ensure the co-ordination of audit efforts to assure the completeness of coverage, reduction of redundant efforts, and the effective use of audit resources?				
3. *a.* Are you satisfied with the knowledge, skills, and abilities of the staff assigned to do the audit work?				
b. Are you satisfied with the engagement leadership assigned, including the partner(s), manager(s) and fieldwork leaders?				
4. *a.* Did the internal auditors work in accordance with agreed audit parameters?				
b. Was co-operative work conducted in a professional manner?				
c. Are you satisfied with the quality and quantity of information provided by the internal auditors?				
5. Are you satisfied that the auditors remain independent of the College in spite of any additional audit-related, or non-audit services the auditors provide to the College?				
6. *a.* Are you aware of any other information that might impair the independence of the internal audit firm?				
b. Are you aware of any individuals on the internal audit team that might not be independent with respect to the College for whatever reason?				

Evaluation of the Internal Auditors	Yes	No	Not sure	Comments
Questions for the Vice Principals and Director of Finance & Estates (continued)				
7. Were identified problems or potential issues brought to your attention in sufficient time to be addressed without delaying or extending the completion of the audit?				
8. *a.* If the choice were yours would you hire the firm to conduct next year's internal audits?				
b. If yes, are there any changes you would make?				

Signed: **Print Name:**

Date:

Standing Items at every Meeting	Minutes of Previous Meeting Schedule of Business Internal Audit (Updates/Reports) External Audit (Updates/Reports) Rolling Audit Action Plan Risk Register KPIs SOFT updates
	Summer Meeting (May / June)
Governance:	Annual Meeting with IA (exc staff) Effectveness Review - committee and IA IA Contract Renewal (June 2028) EA Planning Strategy (current year) IA Reports - HR Systems / Asset Mgt /Governance / Risk IA Final Report current year
Corporate Reporting	ANA / Assurance Map
Student **Learning & Teaching** **People:**	Internal Audit Plan (next acad year)
Annual Updates	Insurance Policy Renewal
Policies:	Complaints Declaration & Management of Interest Safeguarding
Strategies: **Frameworks**	Progress on Strategies
	Autumn Meeting (September)
Governance:	Review of Remit / Membership / Dates of Mtings Draft A&R Com report to Board Draft Annual Report - Review of Corporate Governance Statement Legislative Compliance - Whistleblowing / FOI/DP/H&G/ROIs SFC Accounts Direction for Scotland's Colleges Final IA Annual Report (acad year just ended) Internal Audit Plan (current acad year)(if not June prev)
Student **Learning & Teaching**	IT Security / Controls Report / IT Re-shaping (Disaster Recover Plan -
Finance / Estate/Risk **People:** **Annual Updates**	
Policies: **Strategies:**	IT Admin Sec Policy (Sept 27)
	Joint Meeting with CDC (Nov)
Governance:	Annual meeting with EA (no staff + ARC members only) Report from Audit Committee to Board External Auditor Annual Report & Letter of Rep Financial Statements for the year end & Annual report including Corporate Governance Statement IAs: Student Credits/Funding
Corporate Reporting **Student** **Learning & Teaching**	
Finance / Estate/Risk	Financial Year End Update Management Accounts to Oct Financial Forecast
People:	
Annual Updates	Compliance Report Complaints Report
Policies:	

Strategies:	Progress on Strategies

Spring Meeting (March)

	Additional Items
Governance:	Proposed dates for following year
	IA reports: Staff Rec & Ret; Procurement & Contract Mgt; Financial Controls: Info Sec & IT Cyber Risk
	Annual Review of EA - process
Corporate Reporting	
Students	
Learning & Teaching	
Finance / Estate/Risk	
	PCIP Report (2027)
People:	
Annual Updates	National Fraud Initiative (every 2 years - 2027)
Policies:	
Strategies:	