# Agenda

**20 November 2025**
**AUDIT COMMITTEE**

**S1.20 Stirling Campus, 5.00pm**

**AGENDA**

| | | Publish on Web? | Type | Lead |
|---|---|---|---|---|
| 1 | Annual Report and Financial Statements 2024/25<br>(Joint item with Finance, Resource & Infrastructure Committee) | No | Approval | Senga McKerr |
| | (Paper 1 is withheld from publication on the Forth Valley College website under Section 27 Information Intended for Future Publication of the Freedom of Information (Scotland) Act 2002.) | | | |
| 2 | Draft External Auditors Annual Report to the Board of Management<br>(Joint item with Finance, Resource & Infrastructure Committee) | No | Approval | Mazars |
| | (Paper 2 is withheld from publication on the Forth Valley College website under Section 27 Information Intended for Future Publication of the Freedom of Information (Scotland) Act 2002.) | | | |
| 3 | Apologies, Declaration of Interests and Changes to Members' Register of Interest | N/a | Discussion | Rhona Geisler |
| 4 | Draft Minutes and Matters Arising of meeting of 4 September 2025 | Yes | Approval | Rhona Geisler |
| 5 | Review of Action Tracker | Yes | Discussion | Alison Stewart |
| 6 | Response to Forvis Mazars letter to those charged with Governance | No | Approval | Alison Stewart |
| | (Paper 6 is withheld from publication on the Forth Valley College website under Section 36 Confidentiality of the Freedom of Information (Scotland) Act 2002.) | | | |
| 7 | Policy Approval<br>7.1 IT Security Policy – to follow<br>7.2 AI Policy – to follow | Yes | Approval | Darren Payne |
| 8 | Presentation of Internal Audit Reports<br>8.1 Credits<br>8.2 Student Support Funds<br>8.3 Education Maintenance Allowance | Yes | Discussion | Wbg services |
| 9 | Progress Report on Audit Recommendations | Yes | Discussion | Stephen Jarvie |
| 10 | Risk Management | Yes | Discussion | Alison Stewart |
| 11 | Compliance Report (Complaints, Data Protection and Freedom of Information) | Yes | Discussion | Stephen Jarvie |

| | | | | |
|---|---|---|---|---|
| 12 | Review of Risk | N/a | Discussion | All |
| 13 | Any Other Competent Business | No | Discussion | All |
| 14 | Forward Programme of Committee Business | Yes | Information | Alison Stewart |
| 15 | Three points for Raising with the Board | | Discussion | All |

16. Joint private meeting with auditors and committee members

# 4. Draft Minute of Meeting of Audit Committee

**20 November 2025**
**AUDIT COMMITTEE**

**Falkirk Campus, Steeple Suite, 4.30pm**

Present: Rhona Geisler (Chair)
Lorna Dougall
Grace Hepburn
Suzanne Reynolds

In Attendance: Kenny MacInnes, Principal
Alison Stewart, Vice Principal Finance and Corporate Affairs (VPFACA)
Stephen Pringle, Wbg Services
Michael Speight, Forvis Mazars
Senga McKerr, Head of Finance (HOF) for A/25/004 only
Stephen Jarvie, Corporate Governance and Planning Officer (CGPO)

### A/25/001 Apologies, Declaration of Interests and Changes to Members' Register of Interest

Apologies were noted from Liam McCabe

### A/25/002 Draft Minutes and Matters Arising of meeting of 15 May 2025

Members considered the minute of the meeting of 15 May 2025

Members asked for an update on the Section 22 report.

The VPFACA confirmed that this had been presented to the Scottish Parliament Public Audit Committee who had written to the College requesting further information. She confirmed that a response had been sent and that a copy of the letter would be included in the papers for the Board.

a) Members approved the minute of the meeting.

### A/25/003 Review of Action Tracker

The VPFACA reported that risk management would be covered at the upcoming Board of Management session in September and provided an overview of discussions she and the Chair had had with the external consultant providing the session.

She noted that the action regarding the Principal's objectives being considered by Remuneration Committee was still live.

a) Members noted the content of the update

### A/25/004 National Fraud Initiative 2024-25 Results

The HOF presented a report outlining the latest results from the National Fraud Initiative (NFI) checks for the three-year period to September 2024.

She provided members with an overview of the NFI process which applies across the public sector and the data matching and checks undertaken.

She highlighted that the latest outcomes show that there were no issue or reportable errors identified.

Members queried how often the College has to submit data for the NFI process.

The HOF confirmed that a submission is required every two years but that the submission covers three years of data.

She also discussed how the College systems are designed to identify possible issues and ensure that they are investigated and dealt with when they occur rather than waiting for the NFI checks.

Members welcomed that the team were proactive in this manner.

a) Members noted the content of the report

**A/25/005 Review of Committee Remit**

The VPFACA presented the annual review of the remit of the Committee, noting that it was good practice for members to check the remit each year.

Members commented that the membership section should be updated to reflect that there are now vice-chairs in place for each committee.

The VPFACA confirmed that this change would be made.

Members queried whether the College checked the remits against other Colleges.

The VPFACA noted that this had not occurred since the last major review of all remits Stephen Pringle, WBG Services, noted that the College could send the remits to them for checking if they wanted to.

The VPFCA noted that the Audit Committee Self-Assessment provided a level of assurance that the Committee was covering everything it should or that it was covered by another Committee.

a) Members approved the remit subject to the addition of Vice Chairs

**A/25/006 Audit Needs Assessment**

Stephen Pringle, WBG Service, (SP) presented the annual internal audit plan for the 2025/26 session.

He informed members that the plan had been based on the initial three-year plan and a meeting with the Chair and Vice Chair of the Committee and the VPFACA and Principal.

He outlined revisions to the internal audit standards that apply for the coming year and then provided an overview of the areas to be audited.

Members queried what determines the areas to be audited, and did risk play a part.

SP confirmed that this was the case, with the initial three-year plan being mapped to the College risk register and that current risk registers are reviewed when drafting the plan for the current year, along with the outcome of previous internal audits.

Members noted that the College was entering a period of significant transformation, welcomed that change management was one of the proposed areas for review and that part one of this audit would be undertaken early in the academic year.

a) Members approved the audit needs assessment

**A/25/007** **Governance Statement**

The VPFACA presented the draft governance statement for member's consideration. She highlighted that this forms part of the College accounts and that the current Board membership structure is reflected in the report.

Members noted some small spelling mistakes which would be corrected.

The VPFACA also noted that the upcoming risk management workshop with the Board could form part of the statement and queried the external auditor if this was acceptable. Michael Speight (MS), Mazars confirmed that it would be ok to acknowledge it had occurred post year end as it was a positive development.

a) Members approved the Governance Statement

**A/25/008** **Audit Committee Self-Assessment**

The Chair noted that the document as presented had a number of areas which had been categorised as red in the draft but that this may not be the case and requested members have a discussion on each of these.

Members discussed all the red areas in the draft as presented and made a number of recommended changes.

a) Members approved the self-assessment subject to the changes identified being implemented

**A/25/009 Internal Audit Annual Report**

SP presented the annual report for member's consideration. He outlined the work that had been done and that, in their opinion, sufficient work had been undertaken to allow them to arrive at the conclusion listed in the report.

He noted the number of audits categorised as strong and that, overall when benchmarked against other Colleges, there were fewer recommendations arising from the audit activity than the sector average.

a) Members noted the content of the report

**A/25/010 Presentation of Internal Audit Reports**

**Commercial Income**

SP noted that this should have been presented to the previous committee meeting but that, as no recommendations had been made, this had not had an impact.

a) Members noted the content of the report

**Cyber Security**

SP informed members that the audit had been undertaken by one of WBG Services Cyber specialists owing to the nature of the audit.

He confirmed that the audit mapped the College's performance against the "ten steps of Cyber Security" and that the outcomes were in the report.

Overall, he reported on 5 medium and low-level recommendations and also highlighted that 11 areas of good practice had also been identified.

Members asked the College if further work could be done in the matter of data leak prevention given the upcoming challenges the College is facing and for this to be in place prior to April 2026.

a) Members noted the content of the report

**Sustainability & Carbon Management**

SP reported that this was another audit conducted by a specialist member of their team.

He noted that there were 2 low recommendations made, and 10 areas of good practice identified which was better than the sector average and was quite a strong position for the College to be in going forward.

Members noted their thanks to the teams for delivering this positive position.

a) Members noted the content of the report

**Student Support**

SP reported on the audit of the provision of student support services to students.

He noted that there was only one low grade recommendation, and six areas of good practice identified.

Lorna Dougall commented, as Chair of the Learning & Student Experience Committee, her committee regularly review the support provided but acknowledged, due to ongoing financial constraints, this was an area that could become a risk.

a) Members noted the content of the report

**Follow Up Review**

SP presented the annual follow up review report and outlined progress made by the College against a number of recommendations.

a) Members noted the content of the report

**A/25/011 Progress Report on Audit Recommendations**

The CGPO presented members with a report on the progress against current internal audit recommendations.

Members commented that some recommendations had text stating "No further Updates" and commented that this did not provide much information for the Committee to review. It was suggested that alternate text such as "Recommendation re-examined and progress continuing" may be more useful to members.

Members also commented that updates were particularly important if a recommendation was beyond its recommended implementation date.

In regard to the recommendation on three-year financial forecasts, the VPFACA reported that this would be incorporated into the transformation project and that the next update on progress would reflect that this has been superseded by the transformation project which, in turn would be audited at the appropriate time.

a) Members noted the content of the report

**A/25/012 Risk Management**

The VPFACA presented the risk register to members, noting that there had been some changes since the last meeting.

She confirmed the risks identified at the 14 August Board meeting regarding the three-campus model and the scale of the transformation project had been incorporated into the register.

She also highlighted changes to the presentation of the risk table to make it more user friendly.

She informed members that the College was seeking to remove three risks stemming from the Fuel Change issue as these had now been superseded without reaching fruition.

Members noted that the Board Secretary risk should remain on the register until recruitment for the post is complete. The Principal commented that, should the recruitment not be successful, a shorter-term solution would be pursued.

a) Members noted the content of the report

**A/25/013** **Review of Risk**

The VPFACA noted that, on the risk register, each risk is assigned a Board Committee, and that each Committee should look at their assigned risks. She then outlined the risk relating to the Audit Committee.

a) Members noted the content of the discussion

**A/25/014** **Any Other Competent Business**

**Three Points to Raise to the Board**

The Board Chair has asked that Committees identify three points they would like to bring to the attention of the Board in a single page cover to the Committee minute.

Members agreed that the change to internal audit to include a two-phase change management audit should be included, along with the Annual Report of the Audit Committee and the NFI report.

**Risks to the Board**

Members were asked if there were specific risks to bring to the attention of the Board, there were none identified.

**A/25/015** **Forward Agenda**

The forward agenda was attached for information.

| Meeting | Date | Minute Ref | Action | Assigned to | Deadline to report? | Status | Output Required | Comment |
|---|---|---|---|---|---|---|---|---|
| Audit | 05/09/24 | A/24/013 | College to review the 'treatment' options used for Risk Management to allow for reflection of mitigation. Consider a session with members on risk treatment | Alison Stewart | February Board | Completed | Risk session to be arranged for the Board of Management. | Presented at September 25 Board development day. |
| Audit | 15/5/25 | A/24/039 | Cybersecurity to be included in September risk session as a prominent item | Alison Stewart | 26/09/2025 | In Progress | | Further review of risks being undertaken |
| Audit | 15/5/25 | A/24/040 | Annual calendar of key timelines/milestones within the college | Kenny MacInnes | TBD | In Progress | | Currently work in progress. An update will be brought to the November Audit Committee. |
| Audit | 15/5/25 | A/24/041 | Remuneration committee to be asked to look into staff and student input into the Principal's objectives | Abhi Agarwal/Alison Stewart | TBD | In Progress | Remuneration Committee to consider inputs to Principals' objectives | |

# 7.1 I.T. Security Policy Update
# For Approval

**20 November 2025**
**AUDIT COMMITTEE**

## 1. Purpose

**To seek approval of the amended I.T. Security Policy.**

## 2. Recommendation

That the committee consider and approve the amended I.T. Security Policy

## 3. Background

The security landscape has changed since the policy last went through committee, and there was seen a need to incorporate the mandatory use of staff pictures as a security improvement,

- allowing stronger identity verification in daily operations,
- reducing the risk of internal impersonation or "account hijacking in plain sight".
- improving identity proofing
- decreasing success rates of Business Email Compromise
- improving helpdesk and security operations

Staff and Students can match faces to names, allowing clear identification of speakers or who they met in meetings, improving the integration and efficiency of new staff members. This policy change has been added to section 1.2 of the security procedures document.

This prompted the review of the policy and the following enhancements and changes have been made to the policy.

Guidance and context information has been added

Procedures have been removed from the policy and added to the I.T. Security Procedures document, in line with Forthvalley practice. This document is still in draft, and will change as the security landscape evolves. The procedures document will be ratified by L.M.T. Having the procedures document negates the requirement to continually go through committee with any changes. The draft I.T. Security Procedures Document is included for completeness.

## 4. Actions

A program of policy/procedure awareness raising will be embarked up, with the topic of I.T. Security being added to appropriate college committees and departmental meetings to promote the content, making staff aware of the current and changed security arrangements.

## 5. Resource Implications (Financial, People, Estates and Communications)

I.T. Management time attending meetings to effect awareness raising.

## 6. Equalities

**Assessment in Place? – No**

There are no specific issues in relation to equalities within this paper.

## 7. Communities and Partners

Requirement to be shared with college partners within the buildings. E.g. Skills Development Scotland.

## 8. Risk and Impact

Please complete the risk table below. Risk is scored against Likelihood x Impact, with each category scored from Very Low through to Very High. Risks should be robustly scored and, if the combined score (Likelihood x Impact) is higher than the Board Risk appetite for the risk category identified, additional justification must be provided on why this risk is necessary.

| | Likelihood | Impact |
|---|---|---|
| **Very High (5)** | | |
| **High (4)** | | X |
| **Medium (3)** | X | |
| **Low (2)** | | |
| **Very Low (1)** | | |

**Total Risk Score** – 12

The College has a Strategic Risk appetite for categories of risk as defined by the Board of Management. Decisions being taken at LMT/SMT/Board level must have cognisance of this. Please indicate the single most relevant risk category in the table below.

| BoM Risk Categories & Risk Appetite (Select one area only) | | | | | |
|---|---|---|---|---|---|
| **Cautious <15** | | **Open 15> <20** | | **Eager >20** | |
| Governance | X | Strategy | | People | |
| Legal | | Financial | | Project/Programme | |
| Property | | Reputational | | | |
| | | Technology | | | |

**Is the score above the Board Risk Appetite level?** No

**Risk Owner –** LMT

**Action Owner –** Graeme Robertson

**Paper Author –** Graeme Robertson

**SMT Owner –** Colin McMurray

# 7.1 I.T. Security Policy Update
# For Approval

20 November 2025

AUDIT COMMITTEE

# IT Security Policy

| | | |
|---|---|---|
| Status Approval | Draft | |
| Version Number | 2.6 | |
| Date of Version | November 2025 | |
| Responsibility for Content | ~~IT~~ Head of Information Technology | |
| Responsibility Review | ~~IT~~ Director of Digital Transformation and Innovation | |
| Impact Assessment Review Date | November 2026 | |
| Review Date | November 2026 | |
| Primary Contact | Director of Digital Transformation and Innovation<br>Head of Information Technology | |

## Contents

## 1. Introduction

Forth Valley College (FVC) is committed to ensuring that all information it manages is protected against threats that could compromise confidentiality, undermine integrity, or disrupt availability. In today's digital environment, the FVC's reliance on technology to support all areas across the education arena means that robust IT security is critical to delivering its objectives. Any compromise of systems or data could affect the trust of students, staff, and business partners, disrupt essential services, and expose FVC to legal, regulatory, and reputational risks.

This policy establishes FVC's approach to safeguarding its information and technology resources through established and effective security processes. It provides management direction, sets out responsibilities, and ensures that information security is embedded across all areas of FVC activity. By protecting our digital environment, the FVC not only reduces the risks of cyber threats but also supports innovation, digital transformation, and the safe adoption of new technologies such as cloud platforms and artificial intelligence.

## 2. Scope

This policy applies to all staff, students, delegates, and partners when using Forth Valley College IT infrastructure. It covers all IT systems, devices, networks, cloud services, and emerging technologies, including artificial intelligence. The policy applies to both on-campus and remote access, ensuring that College data and systems remain secure wherever they are used or accessed.

## 3. Principles

Forth Valley College is committed to protecting the confidentiality, integrity, and availability of the information it manages. This principle applies to all data, systems, and services that support learning, teaching, general research (such as business or market), administration, and operations.

The College recognises that reliance on IT systems requires strong and consistent security practices. The objectives of this policy are to ensure that:
All staff, students, contractors, and partners understand their responsibilities in using College IT systems.

Adequate controls and procedures are in place to maintain secure operations and safeguard sensitive information.

All systems and practices comply with relevant legislation, including the Data Protection Act (2018), GDPR, and sector guidance.

These principles are underpinned by effective and established IT security processes, supported by a suite of subsidiary policies and procedures that hold equal standing.

Together they provide a coherent framework for protecting information and ensuring that security is embedded across all College activities.

## 4. What These Principles Mean in Practice

To give effect to these principles, the College maintains a series of operational standards and requirements:

- Physical security ensures that IT equipment is protected against theft and damage, with secure storage, asset registers, and protective tagging in place.

- Logical access controls restrict system access to authorised users with unique accounts, strong passwords, multi-factor authentication, and regular monitoring.

- Backup and contingency planning safeguard against data loss, with daily, weekly, and monthly backups tested regularly and supported by a disaster recovery plan.

- Staff, student and delegate identifiable data must not be stored on removable media.

- Remote access is provided through VPN for legitimate business use, with safeguards for network and data security.

- Wireless networks are restricted to College-owned and approved services such as eduroam, and unauthorised wireless networks and devices are not permitted.

- Asset disposal must follow environmental and data protection regulations and Forth Valley Asset Register procedures with devices securely wiped and disposed of only by accredited appointed providers approved by Forth Valley College, through the I.T. Department.

- Designated secure areas are maintained for critical IT infrastructure across campuses.

By following these standards, the College reduces the risk of breaches, ensures compliance with legal and sector obligations, and maintains trust in its digital environment

## 5. Consultation and Governance

This policy is reviewed by the Digital Steering Group, and approved by the relevant Forth Valley Governing Bodies. Oversight is provided by the Senior Vice Principal for IT,  Director of Digital Transformation and Innovation and Head of IT.

System owners within departments are responsible for ensuring that security requirements are applied consistently to the systems they manage. Staff, students and delegates must comply with this policy and the related procedures, and must seek guidance from IT Services before procuring, deploying, or significantly modifying IT systems, especially those involving cloud services, infrastructure, remote access, or artificial intelligence.

Regular risk assessments will be conducted to determine the appropriate level of security for each system, and independent reviews will ensure compliance and continuous improvement. Breaches of this policy may result in disciplinary action and, where appropriate, reporting to external regulators.

## 6. Useful Resources

Forth Valley College draws on a range of internal and external resources to support effective IT security.

Internally, this policy should be utilised alongside the

- Digital Strategy
- IT Security Procedures
- AI Policy
- AI Procedures
- Acceptable Use Policy
- Data Protection Policy

Externally, the College aligns its practices with sector and regulatory frameworks, including:

- UK National Cyber Security Centre (NCSC) Cyber Essentials
- ISO 27001 Information Security Standard
- Scottish Government Cyber Resilience Strategy
- JISC guidance on information and cyber security in the education sector
- Scottish Environmental Protection Agency (SEPA) requirements for asset disposal

These resources ensure that Forth Valley College remains compliant with legislation, follows sector good practice, and continuously strengthens its information security posture.

# IT Security Procedures

|  |  |
|---|---|
| Status Approval | Draft |
| Version Number | 2.5 |
| Date of Version | November 2025 |
| Responsibility for Content | Head of I.T. |
| Responsibility Review | Head of I.T. / Director of Digital Innovation |
| Review Date | November 2026 |
| Primary Contact | Head of IT |

## Contents

## 1. Introduction

Forth Valley College (FVC) relies on technology to deliver teaching, learning, general research (such as market or business), and administration. These systems and the information they process are critical to FVC's success, but they are also exposed to risks such as unauthorised access, accidental loss, and deliberate cyber-attack. These IT Security Procedures sit beneath the IT Security Policy and translate its high-level commitments into operational practice.

By setting out practical steps for staff, students, delegates, visitors, and business partners, the Procedures explain how FVC's information assets, infrastructure, and services must be protected on a daily basis. Following these procedures ensures consistent security practices across all FVC campuses, supports compliance with legislation such as GDPR, and aligns FVC with good practice from Jisc and the UK National Cyber Security Centre (NCSC),

## 2. Purpose

The purpose of these Procedures is to give clear, actionable guidance that enables FVC community to meet the expectations of the IT Security Policy. They set out the controls required to protect systems and data, explain why these controls matter in reducing risk, and describe how they must be applied in physical, technical, and administrative contexts.

In practice, this means providing direction on matters such as access controls, backups, procurement, cloud use, incident response, and the handling of portable devices. It also means linking IT security with other key areas of governance, including but not limited to the AI Policy and procedures. Together, these policies and procedures ensure that innovation and digital transformation are supported by strong security foundations.

## 3. Scope

These Procedures apply to all members of the FVC community, including staff, students, delegates, visitors, and business partners. They cover all IT systems, networks, devices, and services operated by or on behalf of FVC, whether hosted on-site, in the cloud, or accessed remotely.

This scope also extends to emerging technologies such as AI-enabled platforms, reflecting the need to apply consistent security controls regardless of where or how services are delivered. By applying the same principles across on-campus and remote environments, FVC ensures that information remains protected wherever it is accessed, and that staff and students can work flexibly without compromising security.

For clarity the following definitions are provided on students, delegates and visitors.

Student

- An individual enrolled on an accredited course or programme of study at FVC.
- They have a student record in the FVC student record system, a FVC email address, and long-term access to learning platforms, library resources, and the eduroam Wi-Fi service.

Delegate

- An external participant attending an FVC organised fee-paying course, workshop, or conference e.g. commercial training.
- They are not enrolled as students but are formally registered for a specific event or short-term programme.
- Where delegates are required by their course or workshop to be issued with an aligned student account, to allow access to FVC laptops/pcs, and associated standard software, then the delegate should use the eduroam wi-fi service.
- For security and consistency, delegates who do not require access to FVC laptops/ pc's and associated standard software should use guest Wi-Fi.

·Visitor

- A short-term guest who is not formally enrolled or contracted e.g. external guests attending a one-off meeting.
- Visitors do not have College accounts and should only be provided with guest Wi-Fi for internet access, with no access to internal systems.

## 4. Enforcement and Accountability

Security oversight for these Procedures is provided by the Head of IT, supported by the Systems and Network Officer. Together, they provide direction and visible management support for IT security initiatives.

Responsibility for day-to-day protection of information systems lies with the heads of departments and designated system owners. Each department must ensure that security processes relevant to their systems are carried out consistently and in line with these Procedures. The Systems and Network Officer (or duly appointed alternative role) acts as FVC's central information security role, coordinating technical controls and monitoring.

These Procedures form part of FVC's governance framework and compliance is mandatory. Any breaches may be managed under staff or student conduct regulations as defined by FVC.

To determine the appropriate level of security measures applied to FVC systems, appropriate risk assessments should be conducted. Data Protection Impact Assessments (DPIA) or the successor to of Assessments of High-Risk Processing (AHRP) are to be utilised where personal data is processed. Current guidance from JISC suggest both methods are acceptable. These are currently conducted by the FVC Data Protection Officer (DPO) or now known as Senior Responsible Individual (SRI).

General FVC IT security risk assessments where personal data is not used must be undertaken to identify the likelihood and impact of potential risks and/or failures.

For every new or materially changed system (including web-based software as a solution/Software as a Service (SaaS), the System Owner or Head of Department is accountable for completing and signing off the IT Security Risk Assessment. The IT/Security Team is responsible for providing the template, conducting technical checks, and recommending controls.

Reviews of these risk assessments and the implementation of controls will be carried out to ensure compliance and continuous improvement.

## 5. Core Procedures

The core procedures set out the key security controls that must be applied across FVC. Each procedure outlines the required standard and provides clear guidance to ensure consistent and effective protection of systems, data, and infrastructure.

### 1.1. Physical Security

IT hardware must be protected against theft, loss, or physical damage, because compromised devices may result in data breaches, disruption to services, or reputational damage to FVC. Securing equipment ensures continuity of service and compliance with legal and regulatory requirements.

Procedural Guidance:

- Equipment must be kept in secured areas when not in use.
- Devices handling sensitive data such as CCTV Monitors must be located in separate secure rooms. Approval by the Head of IT must be sought where devices cannot be located in separate secure rooms.
- All IT hardware/Software/Software Licenses must be recorded in FVC's IT asset register.

### 1.2. Logical Access

System access must be controlled to prevent unauthorised use of FVC information and resources. Restricting access reduces the risk of misuse, maintains the integrity of systems, and safeguards personal and sensitive data.

Procedural Guidance:

- Each user must be issued with a unique user ID and password.
- Access should be restricted to the minimum functions required to perform a role.
- Passwords must remain confidential, be updated at agreed intervals, and never shared.
- Passport-style photos will be embedded in FVC systems to support verification of user accounts being accessed by the correct individual.
- Users must log out or lock devices when unattended.
- Only FVC-issued devices may be used for accessing FVC data. The exception to this is one personal mobile phone per staff to access email using multi factor authentication.
- Multi-factor authentication must be enabled wherever possible.
- A Joiner/Mover/Leaver (JML) process must be followed to ensure access is provisioned, updated, or revoked in a timely manner.

- Privileged accounts (e.g. administrative or system-level access) must be separate from standard user accounts and subject to enhanced monitoring and logging.

### 1.3. Backup and Contingency

Regular backups are essential to ensure that College data and applications remain available in the event of system failure, data corruption, or disaster. Backups and contingency planning provide resilience and reduce downtime.

Procedural Guidance:

- Daily, weekly, and monthly backups must be maintained.
- Backup integrity must be tested for both the media and the stored data.
- Backup media must be stored securely in fireproof safes on-site and off-site.
- Weekly, monthly, and annual backups must be retained off-site.
- A Disaster Recovery Plan must be maintained and tested regularly.

### 1.4. Application Purchase, Development and Maintenance

The acquisition and development of IT systems and software must follow secure processes to ensure consistency, compliance, and risk management. Controlling procurement prevents the introduction of unapproved or insecure applications and ensures alignment with FVC policy.

Procedural Guidance:

- All IT procurement must follow FVC's procurement guidance.
- Staff, students, delegates and business partners must comply with the College Acceptable Use Policy.
- Any AI-enabled tools must comply with the AI Policy and follow the relevant AI Procedures
- Where a new or existing system processes personal data, a DPIA (Data protection Impact Assessment)  must be completed and signed off by FVC's DPO  before implementation. It is the responsibility of the Asset Owner implementing the solution to ensure that the FVC DPO is informed and that the DPIA has been completed.
- Where a DPIA is not required, an IT Security Risk Assessment must be undertaken to ensure the system / software is compliant with sector guidance (e.g., Jisc Cyber Security Framework) and that risks are identified, documented, and mitigated. NO digital solution including web based should be used without the appropriate assessment taking place.
- All risk assessments (DPIA  or IT Security Risk Assessment) must be recorded, retained, and reviewed regularly as part of the system's/ software lifecycle management.
- Inhouse developed or externally sourced new or updated applications must be tested for security and compliance prior to release.

- Cloud and Software as a Service (SAAS) services must include security reviews covering tenant configuration, conditional access, data residency, and exit planning.
- Vendor risk assessments must be completed before contracts are signed, including data protection impact, breach notification requirements, and right-to-audit clauses.

### 1.5. Wireless Security

Wireless networks must be carefully managed to protect the integrity and availability of FVC systems. Allowing unapproved devices or unauthorised networks introduces vulnerabilities and can disrupt services. To balance security with accessibility, FVC provides specific wireless networks for different user groups.

Procedural Guidance:

- Students and delegates must connect using the approved service when using their own devices.
- Visitors may use the designated guest Wi-Fi network, which provides internet access without exposing internal FVC systems.
- Wireless access is restricted to FVC-managed networks; unauthorised devices, personal hotspots, or rogue wireless services must not be introduced.

### 1.6. Portable Devices and Removable Media

Portable equipment and removable media present risks of data loss or theft if not properly controlled. Encryption and restrictions are necessary to safeguard sensitive and personal data. This applies not only to USB drives but also to CDs, DVDs, and other physical storage media.

Procedural Guidance:

- All College laptops, hybrid tablets such as MS Surfaces and tablets must use encryption where applicable.
- Staff, students, delegates, visitors, and business partners must not store identifiable FVC data on removable media such as USB sticks, CDs, or DVDs.
- Where removable media is required, it must be encrypted and erased immediately after use.
- All endpoint devices (FVC laptops, surfaces, tablets, and mobile phones) must meet security baselines, including:
  - Regular patching and updates.
  - Anti-malware/endpoint detection and response (EDR).
  - Screen lock and password protection.
  - Device management through FVC approved systems (e.g. Mobile Device Management).

### 1.7. Remote Access

Remote access is necessary for flexible working but must be tightly controlled to protect FVC systems and data. Improper use can expose the network to intrusion or data compromise. Staff must also follow health and safety standards when working remotely to prevent physical risks associated with IT equipment.

Procedural Guidance:

- Remote access is provided only through the FVC VPN.
- Remote access is for legitimate business use only and must not be used for personal activities.
- Staff must ensure secure environments when working remotely and comply with relevant FVC health and safety requirements.
- Only using FVC-supplied power leads.
- Sensitive data must not be stored on non-FVC devices.

### 1.8. Computer Asset Disposal

IT assets must be disposed of securely and sustainably. Improper disposal may result in data breaches or breaches of environmental regulations.

Procedural Guidance:

- All equipment must be securely wiped before disposal.
- Disposal must be handled by IT Services or accredited SEPA-approved providers.
- Duty of care certificates must be retained, and asset registers updated.
- Asset tags must be removed and documented prior to disposal.

### 1.9. Designated Secure Areas

Certain areas of the IT infrastructure require additional security to protect critical systems. Access to these areas is restricted to prevent tampering or misuse.

Procedural Guidance:

- Designated secure areas include computer rooms, node cabinets, and IT build rooms across all campuses.
- Only authorised IT staff may access these areas.

The designated secure areas within the I.T. Infrastructure are as follows.

- Computer Rooms – Falkirk
- I.T. “Build Room” – Falkirk
- All node cabinets – Falkirk
- Computer Room – Alloa
- I.T. Staff Room – Alloa
- Main Node Cabinet Room – Stirling

### 1.10. Network Security

Network infrastructure must be designed and managed securely to protect FVC systems from unauthorised access, data breaches, and service disruption.

Procedural Guidance:

- Firewalls and routers must be securely configured and reviewed regularly.
- Email and web filtering must be applied to protect against malware, phishing, and inappropriate content.
- Remote administration of network devices must be restricted and secured.

## 1.11. Data Classification and Handling

All College data must be classified to ensure it is handled appropriately and consistently. This ensures compliance with legal requirements, reduces risk, and provides clarity on how information should be stored, shared, and disposed of.

AI systems must never be used to process Highly Sensitive data unless explicitly risk assessed and approved.

Procedural Guidance:

Data must be classified into the following categories:

- Public which is information intended for public use (e.g. website content).
- Internal which is routine FVC information for staff, students, delegates, or business partners.
- Confidential which is sensitive operational information requiring controlled access.
- Highly Sensitive which is personal or legally protected data requiring the highest safeguards.

Handling requirements include:

- Encryption for Confidential and Highly Sensitive data.
- Secure sharing via FVC approved systems.
- Prohibition on storing highly sensitive data on removable media or non-FVC devices.
- Secure disposal in line with data protection and SEPA requirements.

## 1.12. Monitoring and Logging

Monitoring activity across FVC systems helps detect and prevent security incidents. Logging provides an audit trail to support investigations and compliance.

Procedural Guidance:

- All IT systems and networks may be logged and monitored.
- Monitoring must follow Jisc and NCSC good practice.
- Logs must be retained in accordance with FVC retention schedules.
- Logs must include, at minimum:
  - Authentication events.
  - Administrative and privileged account activity.
  - Firewall and network security events.
  - Email and web security events.

### 1.13. Incident Response and Escalation

A structured response to security incidents ensures risks are contained quickly and effectively. Clear escalation routes protect FVC from further harm.

Procedural Guidance:

- All incidents must be reported immediately to IT Services.
- Incidents must be managed in line with FVC Cyber Incident Response Plan.
- Lessons learned must be documented and used to strengthen future practices.
- Where incidents involve personal data, the Data Protection Officer (DPO) must be notified as per the FVC Data Protection policy.

### 1.14. Vulnerability and Patch

All IT systems and software can contain weaknesses (known as vulnerabilities) that attackers may exploit. Regular updates, or patches, are issued to fix these issues. To keep FVC systems secure, vulnerabilities must be identified quickly and patches applied within agreed timescales.

The following definitions are used to help assess the different levels of vulnerabilities.

- Critical vulnerabilities are defined as those that can be easily exploited and may cause severe damage, such as complete FVC system compromise or loss of sensitive data.
- High risk vulnerabilities are defined as those that could cause significant disruption or expose important data but may require more effort to exploit.
- Medium risk vulnerabilities are defined as those that pose limited risk on their own but could become serious if combined with other weaknesses.
- Low risk vulnerabilities are defined as minor issues with little or no impact on security, but still worth fixing when practical.

Procedural Guidance:

- Regular vulnerability scans must be performed on FVC systems to identify known weaknesses.
- Critical vulnerabilities must be patched within 14 days, high-risk vulnerabilities within 30 days, medium and low risk as soon as practical.
- Evidence of patching (such as logs, reports, or change records) must be retained for audit and assurance purposes.
- Exceptions to patch timelines must be approved by the Head of IT.

### 1.15. Supplier Risk Management

Vendors provide critical systems and services to FVC, but they also introduce potential risks. Security must be monitored not only at the point of procurement but throughout the lifetime of the relevant contracts where applicable.

Procedural Guidance:

- All suppliers must undergo a risk assessment before contracts are signed, covering data protection, breach notification, and security standards.
- Supplier compliance must be reviewed annually (or more frequently for high-risk services) to ensure standards are maintained.
- Contracts must include the requirement to notify FVC of any data breach or major incident affecting FVC information.
- Where appropriate, the FVC reserves the right to audit suppliers or request independent assurance.

### 1.16. Audit & Review Frequency

Security controls must be regularly tested and reviewed to ensure they remain effective and reflect best practice. Routine checks and independent reviews help identify weaknesses before they are exploited.

FVC is responsible for auditing and reviewing local FVC systems, applications, data handling, and user access, while Jisc manages the security and monitoring of the Janet network infrastructure. The College must ensure it integrates with and complies with Jisc's guidance and reporting requirements.

Procedural Guidance:

- Jisc conducts penetration testing at the Janet network level.
- System access reviews must be carried out at least quarterly by FVC to ensure accounts and permissions remain appropriate for staff, students, delegates, visitors, and business partners.
- FVC must review logs, backups, and configuration compliance for all College-managed systems on a scheduled basis, with evidence retained for audit.
- FVC or the appropriate delegated authority must refresh security risk assessments (including DPIAs / AHRPs where required) when systems undergo major change or at least every two years.

## 6. Roles and Responsibilities

Clear roles and responsibilities are essential to ensuring IT security is consistently applied across FVC. The table below uses the RACI model (Responsible, Accountable, Consulted, Informed) to define expectations:

- Responsible (R): Carries out the activity.
- Accountable (A): Ultimately answerable for the outcome.
- Consulted (C): Provides input, advice, or specialist expertise.
- Informed (I): Kept updated on decisions, progress, or outcomes.

| Activity / Area | SMT | LMT | DDTI | HoIT | SNA | HoD | DPO | S/S |
|---|---|---|---|---|---|---|---|---|
| **Oversight of IT Security Procedures** | C | C | A | R | C | I | C | I |
| **Operational security controls** | I | C | C | A | R | C | I | I |
| **Local compliance & system security** | I | C | C | C | C | R | C | I |
| **Use of AI-enabled tools** | I | C | A | R | C | R | C | I |
| **Risk assessment of systems** | I | C | C | R | R | A | C | I |
| **Incident reporting & escalation** | I | C | C | A | R | R | C | R |
| **Security awareness & training** | I | C | C | A | C | R | C | R |
| **Policy compliance & enforcement** | A | C | R | R | C | R | C | R |

**Key:**

- SMT = Senior Management Team
- LMT = Learning Management Team
- DDTI = Director of Digital Transformation & Innovation
- HoIT = Head of IT
- SNA = Systems & Network Administrator
- HoD = Departmental System Owners (usually Heads of Department)
- DPO = Data Protection Officer
- S/S = Staff and Students

## 7. Training and Awareness

All staff, students and delegates must understand their role in protecting FVC's digital environment. Human error is one of the most common causes of security incidents, and effective training helps to reduce this risk.

Staff, students and delegates who will receive IT security awareness training at induction and through annual refresher sessions. Specialist training will be provided for administrators and departmental system owners who manage higher-risk systems. Training content will evolve to reflect emerging threats and sector guidance from Jisc and the NCSC, ensuring that the FVC community remains alert to new risks.

To build practical awareness, FVC will also run regular phishing simulation tests. These exercises help staff, students and delegates recognise suspicious emails, understand the tactics used by attackers, and practise safe reporting. The purpose of these tests is not to penalise individuals but to strengthen FVC's overall resilience and ensure that any weaknesses are identified and addressed through further training.

## 8. Monitoring and Compliance

IT Services will carry out audits and reviews of compliance with these Procedures. Breaches may result in disciplinary action under FVC's relevant policies and procedures. Audit findings and incident reports will be used to improve resilience.

## 9. Useful Resources

These Procedures are supported by a range of internal and external resources that provide guidance, standards, and frameworks for maintaining robust IT security.

Internal Resources

- IT Security Policy which sets the overarching principles and direction for information security at FVC.
- AI Policy which ensures the safe and responsible adoption of AI-enabled tools in line with FVC values and regulatory requirements.
- AI Procedures which provide operational guidance on the approved use of AI systems within FVC.
- Data Protection Policy which defines how personal and sensitive data must be handled to comply with GDPR and the Data Protection Act (2018).
- Acceptable Use Policy which establishes expectations for the responsible use of FVC IT systems and services.

External Resources

- UK National Cyber Security Centre (NCSC) Cyber Essentials which provides a baseline framework for protecting against common cyber threats.
- ISO 27001 Information Security Standard which sets international best practice for managing information security.
- Scottish Government Cyber Resilience Strategy which supports a resilient public sector approach to cybersecurity.
- Jisc Security Guidance which offers sector-specific advice and benchmarks tailored to further and higher education.
- Scottish Environmental Protection Agency (SEPA) Duty of Care & Waste Management which regulates the secure and environmentally responsible disposal of IT equipment.

# 7.2 AI Policy
# For Approval

20 November 2025
AUDIT COMMITTEE

## 1. Purpose

To seek approval of the Artificial Intelligence (AI) Policy.

The Policy sets the governance framework for responsible, transparent and inclusive AI use across Forth Valley College (FVC).

## 2. Recommendation

That members approve the draft Artificial Intelligence (AI) Policy

## 3. Background

This updated policy provides a principles-led governance framework that is aligned to the revised Digital Strategy 2025–2030 (v5 Draft), and positions FVC as innovative yet safe and compliant.

## 4. Key Considerations

Guidance has been taken from JISC AI policy guidance and other relevant authorities.

The detailed AI procedures will be developed once the policy has been approved. This will take time to ensure it is robust and caters for all the policy requirements.

## 5. Resource Implications (Financial, People, Estates and Communications)

Financial: No direct impact

People: Time for awareness/briefings; targeted CPD on AI literacy (staff and students) and role-specific training for approvers/owners based on the policy.

Estates: No direct impact

Communications: Clear communication and awareness campaigns will be required to embed the policy (and the AI Procedures document when approved) to promote confidence and clarity across students, delegates and staff.

## 6. Equalities

**Who does this impact?**

This Policy is designed to be inclusive and to support equitable access to AI-enabled tools. As a high-level governance document, a separate EqIA is not proposed at policy level; an EqIA will be completed and maintained for the AI Procedures and for any high-risk AI deployments.

**Assessment in Place? – No**

## 7. Communities and Partners

No direct impact will be seen by communities and partners although engagement with sector partners such as JISC and employers will support alignment with AI best practice and ensure FVC remains responsive to wider developments.

## 8. Risk and Impact

Please complete the risk table below. Risk is scored against Likelihood x Impact, with each category scored from Very Low through to Very High. Risks should be robustly scored and, if the combined score (Likelihood x Impact) is higher than the Board Risk appetite for the risk category identified, additional justification must be provided on why this risk is necessary.

If the paper is an approval, please reflect on whether the approval will have any direct or indirect impact for any other areas of operational activity internally or externally within the College – Yes All areas that utilise digital solutions may be impacted by the policy.

| | Likelihood | Impact |
|---|---|---|
| **Very High (5)** | | x |
| **High (4)** | | |
| **Medium (3)** | x | |
| **Low (2)** | | |
| **Very Low (1)** | | |

**Total Risk Score – 15**

The College has a Strategic Risk appetite for categories of risk as defined by the Board of Management. Decisions being taken at LMT/SMT/Board level must have cognisance of this. Please indicate the single most relevant risk category in the table below.

| BoM Risk Categories & Risk Appetite (Select one area only) | | | | | |
|---|---|---|---|---|---|
| **Cautious <15** | | **Open 15> <20** | | **Eager >20** | |
| Governance | | Strategy | | People | |
| Legal | | Financial | | Project/Programme | |
| Property | | Reputational | | | |
| | | Technology | x | | |

The lack of a clear policy (and procedures) could lead to inconsistent or unsafe AI use leading to a reputational risk if academic integrity or data security are compromised. These risks can be mitigated by a clear governance framework (this policy) and operational protocols that will be defined through the AI Procedures.

**Is the score above the Board Risk Appetite level? No**

**Risk Owner –** Colin McMurray
**Paper Author –** Darren Payne

**Action Owner –** Darren Payne
**SMT Owner –** Colin McMurray

# Artificial Intelligence (AI) Policy

| | |
|---|---|
| Status Approval | Draft |
| Version Number | 2.1 |
| Date of Version | November 2025 |
| Responsibility for Content | IT |
| Responsibility Review | Director of Digital Transformation and Innovation |
| Impact Assessment Review Date | June 2026 |
| Review Date | November 2026 |
| Primary Contact | Director of Digital Transformation and Innovation |

To be used in conjunction with AI Procedures, Digital Strategy, IT Security Policy, IT Security Procedures, Data Protection Policy, and IT Acceptable Use Policy.

Contents

## 1. Introduction

Artificial Intelligence (AI) is increasingly embedded in the tools we use every day, ranging from established productivity platforms such as Microsoft Office and emerging digital assistants to advanced generative tools such as ChatGPT and research systems designed to support analysis, modelling, and innovation. These technologies are becoming part of the educational landscape and offer significant opportunities to enhance teaching, learning, assessment, planning, knowledge exchange, and operational efficiency. At the same time, they present important challenges in areas such as academic integrity, data security, accessibility, and ethical use.

Forth Valley College (FVC) is committed to innovation in support of its strategic priorities and mission, while aligning with wider sector ambitions set out by the Scottish Government's digital and education strategies and awarding bodies such as Scottish Funding Council (SFC), JISC and the College Development Network (CDN). AI has the potential to transform how we deliver our curriculum, support our students, and improve the way staff work and collaborate. It can assist with the personalisation of learning, improve inclusivity through adaptive technologies, assist with teaching and assessing along with creating efficiencies in administration and service delivery. For students, AI provides tools that can support their development, employability, and engagement within a digital world. For staff, it offers new methods of learning, managing workload, and exploring creative approaches to teaching and professional practice.

However, AI technologies are evolving at pace. Their rapid development requires careful consideration of risks, limitations, and wider societal and ethical impacts. Concerns include bias within AI systems, challenges to originality and authorship, risks around over-reliance on automated outputs, and the need to protect privacy and sensitive data. The College must therefore ensure that use of AI is framed within a clear set of principles and expectations.

The purpose of this policy is to provide a framework that guides responsible and transparent adoption of AI across FVC. It seeks to maximise the benefits of these tools while safeguarding academic standards, protecting the integrity of learning, teaching and assessing, and ensuring that data is managed securely in line with regulatory requirements. The policy also underlines the College's commitment to inclusivity, accessibility, and ethical practice, ensuring that no student or staff member is disadvantaged by the deployment of AI systems.

This policy applies to all FVC students, delegates, staff, and external partners. It establishes expectations for how AI should be integrated into learning, teaching, assessing and supporting operations. It provides the foundation for related guidance, training, and governance. By setting these standards, FVC affirms its role as a forward-looking institution, embracing innovation while ensuring that technological change is harnessed responsibly, for the benefit of our learners, staff, and the wider communities we serve.

## 2. Scope

This policy is primarily concerned with generative artificial intelligence (AI) and related developments, but it also applies to other forms of AI. It will guide FVC's initial approach to any new and emerging forms of AI.

This policy applies to AI-enabled technologies used for learning, teaching, assessment, planning, administration, and support and covers generative AI tools, AI features in future and existing platforms and other college-approved AI systems.

### 2.1 Generative AI

Generative AI is a subset of AI that specialises in creating new content based on patterns learned from existing data. Key aspects include.

2.1.1 Content creation, the ability to produce text, images, audio, video, and other media. This can enhance teaching resources, automate routine tasks, and provide innovative learning opportunities.

2.1.2 Creative applications, used for tasks like writing, art generation, music composition, and code development. These tools can increase efficiency and creativity for both staff and students but also raise issues around originality and plagiarism.

2.1.3 Underlying technology, often powered by advanced deep learning techniques. Understanding the technology helps us evaluate both the potential and the limitations of generative AI systems.

### 2.2 Artificial Intelligence (AI) – the broader field

AI refers to the wider field of computer science that focuses on creating systems capable of performing tasks that normally require human intelligence. This includes:

2.2.1 Machine learning (ML), enabling systems to improve through experience and adapt to new data without explicit reprogramming.

2.2.2 Natural language processing (NLP), allowing systems to understand, interpret, and generate human language for applications such as chatbots, transcription, and translation.

2.2.3 Computer vision, enabling machines to interpret and process visual information such as images, video, and facial recognition.

2.2.4 Robotics, (including other forms of robotics such as cobots and haptics) applying AI to machines that interact with the physical world, from industrial automation to assistive technologies.

2.2.5 Expert systems, using AI to simulate human decision-making by applying knowledge bases and rules to specific domains.

2.2.6 Generative AI, creating new content such as text, images, audio, video, or code based on patterns learned from existing data, widely used in tools like ChatGPT and Copilot.

2.2.7 Reinforcement learning, training AI systems to make sequences of decisions based on trial-and-error and feedback, important in areas such as adaptive learning and self-driving technologies.

2.2.8 Recommender systems, AI that filters and prioritises information for users, such as recommending courses, resources, or study materials.

2.2.9 Predictive analytics, using AI to forecast outcomes (e.g., student retention risks, resource planning, or performance trends).

### 2.3 Why this matters for Forth Valley College

By recognising the broad range of AI types, the College can set a framework that is not limited to today's tools but applies to current, emerging, and future technologies. AI systems are currently designed to analyse data, recognise patterns, make decisions, complete tasks / actions and solve problems, excelling at tasks such as classification, prediction, and optimisation.

For FVC, this means AI can be harnessed to improve operational efficiency and productivity, personalise learning, and support innovation across learning, teaching, assessing and administration. At the same time, given the pace of change is so immense, these benefits come with risks, including bias, misuse, and data security vulnerabilities. Therefore, AI must always be used in line with safe, legal, ethical, and good practice standards, ensuring its application is responsible, transparent, inclusive, secure, and fully aligned with awarding and governing bodies and the College's mission, values, policies and procedures.

## 3. Principles

FVC commits to a set of overarching principles to guide its use of AI, drawn from sector good practice, in line with awarding and governing body requirements and FVC Quality processes. These principles ensure AI is used to maximise benefits while safeguarding academic integrity, equity, and ethical standards in line with the College's strategy, mission, and values. Underpinning these commitments is the SAFER AI Framework (see Appendix A), which provides the guiding values to ensure that AI adoption at FVC remains **S**ecure, **A**ccountable, **F**air, **E**xplainable, **R**eliable, **A**ccessible, and consistent with **I**ntegrity and compliance.

### 3.1 Forth Valley College Principles

FVC will:

a) Support AI literacy for staff and students by embedding digital and AI skills development into learning, teaching, assessing and supporting functions, ensuring the College community can use AI responsibly, safely, securely, critically, and effectively, and that learners are well-prepared for future careers.

b) Ensure clarity, fairness, and transparency by making clear how AI is used, providing consistent guidance on acceptable behaviours, and applying policies and procedures evenly, so that students and staff can trust and confidently engage with AI systems.

c) Keep policies, procedures and practices under review by adapting them as AI evolves to ensure compliance with legal, ethical, and inclusive standards, and awarding and governing bodies enabling the College to remain agile and responsive rather than constrained by outdated rules.

d) Uphold academic integrity and rigour by maintaining the highest standards of assessment and teaching so that FVC qualifications retain their value and public confidence is protected.

e) Monitor and mitigate discrimination and bias by proactively identifying risks and using AI in ways that enhance equality, diversity, and inclusion.

f) Ensure AI inclusivity and accessibility participation for all and ensure any restrictions do not disadvantage groups relying on accessibility-focused AI.

g) Consider the wider social and environmental impact of AI by taking proportionate action to address sustainability and societal effects, ensuring that FVC remains a socially and environmentally responsible institution and that AI adoption aligns with the college values.

h) Work collaboratively with students, staff, partners and stakeholders to pilot, implement and share good practice, maximise the benefits of AI, and remain aligned with awarding and governing bodies both nationally (and internationally where applicable) so that innovation is accelerated, duplication of effort is avoided, and the College can learn from others' experience.

### 3.2 Staff AI Principles

All staff (including but not limited to lecturers, associate trainers, bank and corporate services) at FVC must use AI responsibly and in line with the College's values, policies and procedures. This means acting ethically, respecting data and confidentiality, safeguarding academic integrity, and supporting inclusivity and sustainability in their work.

The AI Procedures document provides detailed operational guidance for staff, including but not limited to expectations around secure data use, teaching, assessing, transparency, and collaboration.

All Staff must;

a) Respect data and ethical standards: do not input personal, sensitive, student, or College information into unapproved AI tools. Ensure all AI use complies with FVC procedures, data protection, confidentiality requirements, and ethical standards. Provide clear guidance to students on safe and responsible practice.

b) Develop and share AI skills: engage with training and guidance to build AI literacy, use tools responsibly and critically, and support students and delegates in developing future-ready skills.

c) Be clear and transparent: explain how AI is being used in teaching, assessment or professional services, so that colleagues, students and delegates can trust decisions and understand expectations.

d) Safeguard academic integrity: In line with awarding and governing bodies, design assessments and teaching approaches that uphold originality and rigour, making clear to students when AI use is appropriate and when it is not.

e) Promote fairness and inclusion: use AI in ways that reduce barriers, challenge bias, and create accessible learning and working environments, ensuring all students and staff are treated equitably.

f) Consider wider impacts: reflect on the social and environmental implications of AI in teaching and operations and adopt practices that align with the College's commitments to responsibility and sustainability.

g) Work collaboratively: share good practice with colleagues, partners, and awarding and governing bodies, ensuring FVC remains aligned with sector standards and able to adapt quickly to emerging developments.

### 3.3 Student and Delegate AI Principles

Whilst utilising FVC infrastructure, all students and delegates must use AI responsibly, transparently, and in line with the College's values, policies, and programme-specific guidance. They must uphold academic integrity and ensure their work reflects their own thinking and achievement.

Students and delegates must:

a) Respect data and ethical standards: do not input personal, sensitive, or College information into unapproved AI tools. Always follow College guidance on safe and ethical use.

b) Build AI skills: use College guidance and training to develop understanding of AI, so it can be used responsibly, critically, and effectively in studies and future career opportunities.

c) Be clear and transparent: The use of AI should be  acknowledged if it has been used to create a response to an assessment either formative or summative, and the details should be recorded in an appropriate way.

d) Protect academic integrity: do not use AI to misrepresent assessed coursework as personal achievement. Ensure submissions reflect original thinking and meet the highest academic standards as defined by the awarding and governing bodies.

e) Challenge bias and be inclusive: use AI in ways that support fairness, diversity, and accessibility, and report any concerns about discrimination or unfairness.

f) Consider wider impacts: remember that AI has social and environmental effects. Use it responsibly, in ways that support both learning and the College's wider commitment to sustainability.

g) Work with others: engage in discussions with lecturers, peers, student partnerships, College forums, and approved partners/ groups to share good practice, learn from each other, and stay up to date as AI evolves.

i) Not use AI systems to create or disseminate content that is abusive, harassing,
discriminatory or otherwise harmful, as defined by the relevant FVC Safeguarding and Disciplinary policies.

## 4. What These Principles Mean in Practice

### 4.1 Working Collaboratively

FVC will engage with students, delegates, staff, partners, employers, professional bodies, and sector experts to share good practice and ensure our approach to AI is interdisciplinary and future-facing.

### 4.2 Supporting AI Literacy

The College will build student, delegate and staff AI literacy through training, guidance, and resources. Understanding both the opportunities and the limitations of AI is essential so that our community can use these tools responsibly, critically, and effectively in learning, teaching, assessing and supporting corporate services.

Developing AI literacy at FVC means:

a) All students and delegates gain skills to use AI appropriately during their studies and future careers.
b) All teaching and associate training staff can adapt teaching methods, assessment design, and research/ planning approaches to incorporate AI, where beneficial and in line with awarding and governing bodies.
c) Corporate services staff can use AI to improve processes while understanding its limits.

AI literacy will be supported across all areas of learning and teaching, including through the progressive integration of AI-related knowledge and skills within curriculum design. This includes consideration of regional economic priorities, such as manufacturing, energy and logistics, to ensure learners develop the competencies required by industry.

Key areas of awareness include privacy, data protection, information security, bias and discrimination, accuracy and reliability, copyright and ethical use, and potential risks of exploitation in AI development.

### 4.3 Clarity, Fairness, and Transparency

The College will ensure AI is used in ways that are open, fair, and easy to understand. Transparency matters because it builds trust, allows users to know how AI is influencing decisions, and ensures no group is unfairly advantaged or disadvantaged.

### 4.4 Regular Review of Policies, Procedures and Practices

AI technologies are developing quickly. The College will keep its policies, procedures, teaching practices, and services under regular review to ensure they remain legal, ethical, and inclusive. This matters because outdated rules risk either blocking innovation or failing to protect against harm. Specific and detailed AI related procedures shall be noted in the AI Procedures document.

### 4.5 Academic Integrity and Rigour

The College will uphold high standards of academic integrity in line with awarding and governing body requirements and FVC Quality processes by students, delegates and staff to use AI ethically in learning, teaching, and assessment. This matters because protecting fairness and originality safeguards the value of FVC qualifications and prepares learners for real-world AI use.

### 4.6 Equity and Inclusion

The College will take reasonable steps to identify and mitigate potential inequities arising from AI use, ensuring fair and inclusive access and avoiding disproportionate impacts on any group of learners or staff. This matters because AI should reduce barriers to learning, not reinforce them, and the College must ensure all students, delegates and staff have equitable access to the tools they need.

### 4.7 Wider Social and Environmental Impact

The College will consider the broader social and environmental effects of AI use, including sustainability and unforeseen impacts. This matters because FVC is committed to social responsibility, and decisions about AI adoption must align with our values and our duty to future generations.

## 5. Consultation and Governance

Students, delegates and staff must seek appropriate guidance as defined by the relevant FVC policies and procedures before using AI in any context where risks may arise around data, academic standards, confidentiality, or compliance. Seeking advice ensures that AI is used responsibly, that the College meets its legal and regulatory obligations, is aligned with awarding and governing bodies and that FVC is protected from reputational, financial, or ethical harm.

The AI Policy establishes this principle of consultation as part of good governance. The implementation of this Policy is supported by associated AI Procedures, the Digital Strategy 2025–2030, and relevant College governance frameworks.

## 6. Useful Resources

Forth Valley College will ensure that staff and students have access to up-to-date resources and sector guidance on the safe and effective use of AI. FVC reference points include but not limited to.

a) AI Procedures
b) IT Security Policy
c) IT Security Procedures
d) IT Acceptable Use Policy
e) Equality, Diversity & Inclusion Policy

For clarity the following definitions are provided on students and delegates.

Student

- An individual enrolled on an accredited course or programme of study at FVC.
- They have a student record in the FVC student record system, a FVC email address, and long-term access to learning platforms, library resources, and the eduroam Wi-Fi service.

Delegate

- An external participant attending an FVC organised fee-paying course, workshop, or conference e.g. commercial training.
- They are not enrolled as students but are formally registered for a specific event or short-term programme.

External reference points used within this policy include the following, noting this is not an exhaustive list.

JISC

College Guidance on creating AI policy Considerations on wording when creating advice or policy on AI use

Security AI and Data Security – Let's Worry About the Right Things

HE examples Navigating the Future: Higher Education policies and guidance on generative AI

AI maturity toolkit for tertiary education

## Appendix A: SAFER AI Framework

The SAFER AI Framework has been developed by Forth Valley College with reference to national and sector guidance, including resources from Jisc's National Centre for AI and relevant Scottish Government and Scottish Funding Council publications.

Forth Valley College adopts the SAFER AI Framework to guide all use of artificial intelligence. This framework provides a set of principles that underpin responsible adoption, ensuring AI use aligns with college values, sector best practice, and legal/ethical requirements. These principles inform the AI Procedures and must be considered in all decisions relating to AI.

| # | Principle | Description |
|---|---|---|
| **S** | Security & Privacy | Protect sensitive data and ensure AI tools meet GDPR, encryption, and vendor due diligence standards. |
| **A** | Accountability | Ensure humans remain in control of AI outcomes through governance and staff CPD so that oversight is informed and effective. |
| **F** | Fairness | Guarantee equitable access to AI tools, skills, and employability outcomes, ensuring all students are workforce-ready and no group is disadvantaged. |
| **E** | Explainability & Transparency | Ensure AI use is understandable, open to scrutiny, and used as a springboard for innovation and creativity, with clear communication of how creative outputs are generated and evaluated. |
| **R** | Reliability & Safety | Require AI tools to be tested for accuracy, quality, and safety in for college use, assessing data input and delivering outputs that are not only safe but also creative, high-quality, and non-generic. |
| **A** | Accessibility & Inclusiveness | Ensure AI-enabled education is accessible to all, regardless of ability or background, and supports employability by ensuring all learners develop AI fluency for the future workplace. |
| **I** | Integrity & Compliance | Align AI use with laws, ethics, sustainability, and College values, including a commitment to environmental sustainability, responsible vendor practices, and green AI to reduce waste and energy use. |

wbg

# Forth Valley College

Credits Audit 2024/25
September 2025

# Table of contents

**Section** **Page**

**Appendix** **Page**

*The matters raised in this report came to our attention during the course of our audit and are not necessarily a comprehensive statement of all weaknesses that exist or all improvements that might be made.*

*This report has been prepared solely for Forth Valley College's individual use and should not be quoted in whole or in part without prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any third party.*
*We emphasise that the responsibility for a sound system of internal control rests with management and work performed by internal audit should not be relied upon to identify all system weaknesses that may exist. Neither should internal audit be relied upon to identify all circumstances of fraud or irregularity should there be any although our audit procedures are designed so that any material irregularity has a reasonable probability of discovery. Every sound system of control may not be proof against collusive fraud. Internal audit procedures are designed to focus on areas that are considered to be of greatest risk and significance.*

# 1 Executive Summary

## Introduction

A review of the College's student data returns has been carried out in accordance with the "Credit Guidance for Colleges AY 2024-25" issued by the Scottish Funding Council (SFC) on 26 June 2024 and the "FES Return and Audit Guidance 2024-25" issued 13 August 2025.

The audit certificate, along with the College certificate, was submitted to the Scottish Funding Council on 3 October 2025. This report was submitted to the SFC on 3 October 2025.

## Scope of Review

The audit procedures have been designed to ensure the College has adhered to the "Credit Guidance for Colleges AY 2024/25". As planned, the audit took 5 days to complete comprising fieldwork carried out by the Auditor and a review by the Manager, Director, and the Partner. All staff involved in the audit had relevant experience.

Our audit sample was selected using analytical techniques and covered a minimum of 5% of the total Credits count with a minimum of 15 courses being tested. Additional sample checks were also carried out on Credits relating to Infill courses/students, Credits spanning academic years, Fee Waiver, and non-fundable courses/students.

The audit process of reviewing the returns being submitted was carried out using the following processes:

- A review of the systems operated by the College for the return;
- Appropriate walk through and compliance checks for the relevant areas;
- Analytical review techniques to ensure testing was undertaken in the most appropriate areas;
- Reviewing the risk areas, issues raised in 2023/24 and the specific issues for 2024/25 highlighted in the audit guidance;
- Sample checking the data included in the return; and
- Specifically tailored Credits audit programmes.

# 1 Executive Summary

## Summary of Recommendations

### Current Year recommendations

| Grading of Recommendations | High | Medium | Low | Total |
|---|---|---|---|---|
| Credits | - | - | 2 | 2 |

### Prior Year recommendations

| Grading of recommendations | High | Medium | Low | Total |
|---|---|---|---|---|
| Fully Implemented | - | - | 1 | 1 |
| Superseded | - | - | 1 | 1 |
| **Total** | **-** | **-** | **2** | **2** |

We have not included the fully implemented recommendation as an appendix; however, details of this recommendation are available upon request.

# 1 Executive Summary

## Conclusion

### Overall conclusion

The audit certificate in respect of the 2024/25 return included within Appendix A, is unqualified and is in the format set out in the SFC audit guidance. The audit certificate was submitted to SFC on 3 October 2025.

| Overall Conclusion: |
|---|
| The College has reasonable procedures and controls over the collection of data for the credits return and assurance can be taken that the credits count for the College is not materially mis-stated. The systems used by the College are satisfactory. The recommendations arising as a result of our review are included within **Appendix C**.<br>We were able to confirm that one of the two recommendations raised in 2023/24 have been implemented with the other raised again this year. We have raised two low grade recommendations for improvement for 2024/25.<br>The College's credit target for the academic year 2024/25, agreed between the SFC and the College, was 79,107. The total credits claimed for the year was 77,785. |

| | Target | Claimed | Variance |
|---|---|---|---|
| Total Credits | 79,107 | 77,785 | 1,322 |

As can be seen from the above table, the College has exceeded its credits target for 2024/25.

# 2 Benchmarking

We include for your reference comparative benchmarking data of the number and ranking of recommendations made for audits of a similar nature in the year ending 31 July 2024.

## Credits Audit 2024/25

| Benchmarking | High | Medium | Low | Total |
|---|---|---|---|---|
| Average number of recommendations in similar audits | - | 1 | 1 | 2 |
| Number of recommendations at Forth Valley College for 2024/25 | - | - | 2 | 2 |

From the table above it can be seen that the College has a similar number of recommendations compared to those colleges it has been benchmarked against.

# 3 Risk Areas and Audit Tests

## Non-Fundable Activity

We reviewed, in full, with the College to confirm that all activity which has been classified as fundable has been correctly classified. We reviewed non-fundable activity to assess whether this is complete. ***From our review, we found that all courses were accurately treated as either fundable or non-fundable by the College.***

## Non-Fundable and Fundable Students

We reviewed, in full, all students classified as non-fundable by the College to confirm accuracy and completeness.  Testing was performed to ensure that credits values have only been allocated to fundable students. ***Our testing indicated that the College were incorrectly not claiming credits for one student. Please see Appendix C: Current Year Recommendations for further information.***

## Full-Time and Other than Full-Time Classification

A sample of 15 courses, covering 5.1% of total credits, were randomly selected from the two modes of attendance. Testing was undertaken to ensure these were correctly classified. ***We can conclude that all courses tested were correctly classified.***

## Infill Students

The word 'infill' appears in the title of courses if they are an infill course. The College have 16 infill courses. We tested a sample of 10 students treated as infilling into courses to assess whether they had been correctly classified, and that credits had been calculated correctly. We also reviewed in full the students the College were classifying as infill students to confirm that credits were only being claimed for the subjects the students had undertaken. ***No issues were found from our testing.***

## Attendance Criteria

For our sample of 15 courses tested (5.1% of total credits claimed), we checked to assess whether the College had correctly calculated and recorded the required date. ***We can confirm that the College has calculated course required dates in line with the guidance.***

# 3 Risk Areas and Audit Tests

For a total of 25 students, we assessed whether the College had obtained a valid enrolment form. ***We can confirm that for each student in our sample an appropriate enrolment record was available.***

We traced a total of 25 students to attendance registers to assess whether they had attended beyond the required date, where credits had been claimed for the student. ***We can confirm that each student in our sample was appropriately traced to the attendance register.***

We also performed testing on a sample of 10 withdrawals (withdrawn within 2 weeks of the required date) to assess whether these had been processed in accordance with SFC guidance. ***No issues found.***

## Credits Count

For our sample of 15 courses, we recalculated the individual credits for each of these courses to confirm the correct value had been allocated by the College. We reviewed the attendance of the students on these courses to assess whether credits were only attributed to those students who had attended beyond the required date and who were fundable students. ***No issues found.***

## Maximum Credits Claim

All students with more than one enrolment were identified and investigated to ensure credits were not overclaimed. ***Our testing found that there were no overclaims as a result of students having more than one enrolment.***

## Average Credits

We confirmed that the average number of credits for FE full time students was 16.83 and for HE full time students was 14.28. This is in line with the SFC guidance.

## Fee Waiver

A random sample of 10 fee waived students were selected (excluding automatic fee waivers). We checked to assess whether their eligibility for a fee waiver had been assessed appropriately by the College. This was done by tracing to an enrolment form and where appropriate a fee waiver form and relevant eligibility documentation. We also assessed whether the students had been allocated to the most appropriate fee waiver category. ***We found that there were issues with fee waiver students surrounding wrongly coded fee waivers, and fee waiver documentation retainment. As a result of these findings, please see Appendix C: Current Year Recommendations for further information.***

## Distance Learning

The College did not have any distance learning courses for the 2024/25 academic year, this was identified during our analysis of the FES and confirmed by the College.

# 4 Audit Arrangements

The table below details the actual dates for our fieldwork and the reporting on the audit area under review.

| Audit stage | Date |
|---|---|
| Fieldwork start | 15 September 2025 |
| Closing meeting | 23 September 2025 |
| Draft report issued | 26 September 2025 |
| Receipt of management responses | 3 October 2025 |
| Final report issued | 3 October 2025 |
| Submission to the SFC | 3 October 2025 |
| Audit Committee | 20 November 2025 |
| Number of audit days | 5 |

# 5 Key Personnel

We detail below our staff who undertook the review together with the College staff we spoke to during our review.

| Wbg | | | |
|---|---|---|---|
| Partner | Graham Gillespie | Partner & Head of Internal Audit | gg@wbg.co.uk |
| Director | Stephen Pringle | Director of Internal Audit | sp@wbg.co.uk |
| Manager | Siobhan Archibald | Internal Audit Manager | sma@wbg.co.uk |
| Senior | Kyle McGuiness | Internal Audit Senior | kmg@wbg.co.uk |
| Auditor | Oliver McLaughlin | Internal Auditor | oml@wbg.co.uk |

| Forth Valley College | | | |
|---|---|---|---|
| Key Contacts: | Lesley Burn | Data Manager | lesley.burn@forthvalley.ac.uk |
| | Lyndsay Condie | Director of Operations | lyndsay.condie@forthvalley.ac.uk |
| Wbg appreciates the time provided by all the individuals involved in this review and would like to thank them for their assistance and co-operation. | | | |

# Appendices

# A. Audit Certificate

## Auditors' Report to the members of the Board of Management of Forth Valley College

We have audited the FES return which has been prepared by Forth Valley College under the SFC's Credits Guidance for colleges issued 26 June 2024 and which has been confirmed as being free from material misstatement by the College's Principal in her Certificate dated 3 October 2025.

We conducted our audit in accordance with the 2024-25 audit guidance for colleges. The audit included an examination of the procedures and controls relevant to the collection and recording of student data. We evaluated the adequacy of these controls in ensuring the accuracy of data.  It also included examination of evidence relevant to the figures recorded in the student data returns. We obtained sufficient evidence to give us reasonable assurance that the returns are free from material misstatement.

In our opinion:

- The student data returns have been compiled in accordance with all relevant guidance;
- Adequate procedures are in place to ensure the accurate collection and recording of the data; and
- Subject to the exceptions noted in this report, we can provide reasonable assurance that the FES return is free from material misstatement.

Signature

| | |
|---|---|
| Date | 3 October 2025 |
| Name of Audit Firm | Wbg Services LLP |
| Contact Name | Graham Gillespie |
| Contact telephone number | 0141 566 7000 |

| | |
|---|---|
| Date FES returned | 3 October 2025 |

wbg

# B. Summary of Errors

The table below highlights the value of credit errors that the auditor found during the course of the audit and notes that these errors were subsequently corrected in the SFC FES return.

| Summary of Error | Number of Raw Credits | Adjusted/Unadjusted in FES Return |
|---|---|---|
| Credits not claimed when the students were eligible for them. | 2.7 | Adjusted |
| **Total** | **2.7** | |

# C. Current Year Recommendations

## Inaccuracies in Fee Waiver Coding and Supporting Evidence

| Ref. | Finding and Risk | Grade | Recommendation |
|---|---|---|---|
| 1. | Fee waiver eligibility should be determined by the College through a clear and consistent process. Students are expected to provide accurate information on their fee waiver forms, and the College should verify this against appropriate supporting evidence before confirming the fee waiver code. The fee waiver code recorded in student records and on the FES 2 return must accurately reflect the student's circumstances to ensure correct funding claims and avoid duplication.<br>During our review, we complete sample testing of 10 students with fee waivers which identified multiple issues. In two cases, the student had been incorrectly coded by the College, which was subsequently amended. Additionally, for a further two students coded as fee waiver 49, 'Asylum seeker or spouse or child of an asylum seeker', we could not evidence source documentation to confirm their status. We were informed that the documents are held but due to an upgrade to Office 365, the evidence cannot be accessed.<br>Failure to apply correct fee waiver codes increases the risk of inaccurate FES 2 reporting and inappropriate funding claims. This exposes the College to the risk of funding clawback, potential financial loss where claims are deemed ineligible, and reputational risk. | **Low** | We recommend that the College strengthen its fee waiver process by conducting periodic checks on student fee waiver codes. A formal review process should be introduced so that any discrepancies between student declarations, fee waiver forms, and enrolment records are identified and resolved prior to submission of FES 2 returns. Additionally, the College should ensure source evidence is stored appropriately to support funding decisions. |

# C. Current Year Recommendations

| Management response | Responsibility and implementation date |
|---|---|
| Forth Valley College acknowledges the recommendation and agrees that enhancing the fee waiver process is essential to ensure accuracy and compliance with funding requirements. The College will implement a formal review mechanism to periodically verify student fee waiver codes against declarations, fee waiver forms, and enrolment records. This review will be scheduled prior to the submission of FES 2 returns to ensure any discrepancies are identified and resolved in a timely manner.<br>Additionally, procedures will be updated to ensure that all source evidence supporting fee waiver decisions is stored securely and is readily accessible for audit and verification purposes. Training will be provided to relevant staff to reinforce the importance of documentation and compliance with funding guidelines. | *Responsible Officer: Lyndsay Condie*<br>*Implementation Date: March 2026* |

# C. Current Year Recommendations

| Fundable students | | | |
|---|---|---|---|
| Ref. | Finding and Risk | Grade | Recommendation |
| 2. | The College's FES submission process requires that all students' records are accurate and complete before submission to ensure proper allocation of SFC credits. Late changes or corrections should be documented, justified, and verified before being included in revised submissions.<br>During our review, it was found that one student, within our sample that qualified for funding on the original FES provided had 0 credits claimed. When queried with the College, it was identified that credits should have been claimed for the students identified, where the student had been noted as 'potentially to be cancelled', with credits removed; however, the new enrolment was not subsequently updated. The College has since claimed 2.7 credits for the student in a revised FES.<br>This finding is similar to one raised during our 2023/24 credits review and as such the previous finding has been superseded.<br>Failure to record enrolment data accurately increases the risk of credits being understated, which may lead to a loss of funding. | Low | We recommend that care is taken when inputting data into the FES so that credits are appropriately claimed, and the College receives its full entitlement. Where late adjustments are made, these should be reviewed in full to ensure no underclaims or overclaims are missed. |

# C. Current Year Recommendations

| Management response | Responsibility and implementation date |
|---|---|
| Forth Valley College acknowledges the importance of accurate data input into the FES system to ensure that credits are appropriately claimed and the College receives its full funding entitlement. To address this recommendation, the College will reinforce existing data validation procedures and introduce an additional layer of review for late adjustments to ensure all changes are thoroughly checked for potential underclaims or overclaims.<br>Staff involved in FES submissions will receive updated guidance and training to support accurate data entry and to highlight the importance of timely and complete reviews of any post-submission amendments. The College will also explore opportunities to strengthen system controls and reporting tools to support proactive identification of discrepancies.<br>These actions will help safeguard the integrity of FES returns and ensure the College maximises its funding in line with regulatory requirements. | *Responsible Officer: Lyndsay Condie*<br>*Implementation Date: March 2026* |

# D. Prior Year Recommendations

## Superseded

| Fee Waiver: Source of Finance | | | |
|---|---|---|---|
| **Original Finding**<br>The College's FES submission process requires that all students' records are accurate and complete before submission to ensure proper allocation of SFC credits. Late changes or corrections should be documented, justified, and verified before being included in revised submissions.<br>During our review, it was found that 14 students that qualified for funding on the original FES provided had 0 credits claimed. When queried with the College, it was identified that credits should have been claimed for the students identified. The College has since claimed 7.1 credits for the student in a revised FES.<br>There is a risk that the College are underclaiming their credits.<br>**Original Recommendation**<br>We recommend that care is taken when inputting data into the FES so that credits are appropriately claimed, and the College receives its full entitlement. | | | |
| Ref. | Finding and Risk | Grade | Recommendation |
| 1. | As a result of our findings identified for 2024/25, it was agreed to supersede this recommendation. | **Low** | No further action required |

# E. Grading Structure

For each recommendation, we assign a grading either as High, Medium or Low priority depending on the degree of risk assessed as outlined below:

| Grading | Classification |
|---|---|
| High | Major weakness that we consider needs to be brought to the attention of the Audit Committee and addressed by Senior Management of the College as a matter of urgency. |
| Medium | Significant issue or weakness which should be addressed by the College as soon as possible. |
| Low | Minor issue or weakness reported where Management may wish to consider our recommendation. |

wbg

# Forth Valley College

Student Support Funds 2024/25

September 2025

# Table of Contents

# Disclaimer

wbg

*The matters raised in this report came to our attention during the course of our audit and are not necessarily a comprehensive statement of all weaknesses that exist or all improvements that might be made.*

*This report has been prepared solely for Forth Valley College's individual use and should not be quoted in whole or in part without prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any third party.*

*We emphasise that the responsibility for a sound system of internal control rests with management and work performed by internal audit should not be relied upon to identify all system weaknesses that may exist. Neither should internal audit be relied upon to identify all circumstances of fraud or irregularity should there be any although our audit procedures are designed so that any material irregularity has a reasonable probability of discovery. Even sound systems of control may not be proof against collusive fraud. Internal audit procedures are designed to focus on areas that are considered to be of greatest risk and significance.*

# 1. Executive Summary

### Introduction

This report has been prepared following the conclusion of our audit of the Student Support Funds for the year ended 31 July 2025.

The audit certificate for the Scottish Funding Council (SFC) funds was submitted on 3 October 2025.

### Summary of Recommendations

| Current Year Recommendations | High | Medium | Low | Total |
|---|---|---|---|---|
| SSF Audit 2024/25 | - | - | 2 | **2** |

| Prior Year Recommendations | High | Medium | Low | Total |
|---|---|---|---|---|
| Fully Implemented | - | - | 1 | **1** |

We have not included fully implemented recommendations as an appendix; however, details of these recommendations are available upon request.

# 1. Executive Summary

## Conclusion

| Overall Conclusion: |
|---|
| We have examined the records of Forth Valley College and have obtained such explanations and carried out such tests as we considered necessary. On the basis of our examination and of the explanations given to us, we report that the information set out in these forms is in agreement with the underlying records. We also report that, in our opinion, the College used these funds in accordance with the guidance issued by the Scottish Funding Council. We are satisfied that the systems and controls of the administration and disbursement of these funds are adequate.<br>We can confirm that all recommendations raised in 2023/24 have been fully implemented, however two new recommendations have been raised in respect of our 2024/25 audit. |

# 1. Executive Summary

### Summary of Income & Expenditure

The table below provides a summary of the income and expenditure for each of the funds and provides details of the fund position at the end of the year. Further detail on the expenditure incurred by fund can be found at Appendix A.

| | SFC | | | | | SAAS |
|---|---|---|---|---|---|---|
| | **Bursary** | **Discretionary** | **Childcare** | **Total** | | **HE Discretionary** |
| Income | 2,877,053 | 273,071 | 137,495 | **3,287,619** | | 93,193 |
| Expenditure | 2,817,452 | 273,071 | 137,495 | **3,228,080** | | 91,250 |
| **Under/(Over) Spend** | **59,601** | **-** | **-** | **59,601** | | **1,943** |

As can be seen from the above table, the College has an underspend on its student support funds of £59,601, which will need to be returned to the SFC.

# 2. Benchmarking

We include for your reference comparative benchmarking data of the number and ranking of recommendations made for audits of a similar nature in the year ending 31 July 2024.

| Benchmarking | High | Medium | Low | Total |
|---|---|---|---|---|
| Average no. recommendations in similar audits | - | 1 | 1 | 2 |
| Recommendations at Forth Valley College | - | - | 2 | 2 |

As can be seen from the above table, the College has a similar number of recommendations in comparison to the colleges it has been benchmarked against.

# 3. Audit Arrangements

The table below details the dates of our fieldwork and the reporting of the audit area under review.

| Audit Stage | Date |
|---|---|
| Fieldwork start | 8 September 2025 |
| Closing meeting | 19 September 2025 |
| Draft report issued | 26 September 2025 |
| Receipt of management responses | 30 September 2025 |
| Final report issued | 1 October 2025 |
| Submission to Scottish Funding Council | 3 October 2025 |
| Audit Committee | 20 November 2025 |
| No of audit days | 4 |

# 3. Audit Arrangements

We detail below our staff who undertook the review together with the College staff we spoke to during our review.

| Wbg Services LLP | | | |
|---|---|---|---|
| Partner | Graham Gillespie | Partner and Head of Internal Audit | gg@wbg.co.uk |
| Director | Stephen Pringle | Director of Internal Audit | sp@wbg.co.uk |
| Manager | Siobhan Archibald | Internal Audit Manager | sma@wbg.co.uk |
| Senior | Kyle McGuiness | Internal Audit Senior | kmg@wbg.co.uk |

| Forth Valley College | | | |
|---|---|---|---|
| Key Contact: | Allison Hewitt | Systems and Management Accountant | allison.hewitt@forthvalley.ac.uk |

Wbg appreciates the time provided by all the individuals involved in this review and would like to thank them for their assistance and co-operation.

# A. Summary of Returns

**Scottish Funding Council Return**

| Bursary Student Numbers & Expenditure | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Students u18 | | Parentally Supported (At Home) | | Parentally Supported (Away from Home) | | Self-Supporting | |
| | **Students** | **£** | **Students** | **£** | **Students** | **£** | **Students** | **£** |
| Maintenance Allowances: | - | - | 230 | 747709 | 4 | 12,167 | 120 | 520,578 |
| Residence Costs | - | - | - | - | - | - | - | - |
| Dependents Allowance | - | - | - | - | - | - | - | - |
| Study Expenses Allowance | - | - | 83 | 9,285 | 2 | 336 | 31 | 5,024 |
| Travel Expenses Allowance | - | - | 21 | 16,953 | 1 | 563 | 85 | 60,389 |
| Additional Support Needs Allowance | - | - | 2 | 3,350 | - | - | 2 | 537 |
| **Total Numbers & Spend** | - | - | 231 | 777,297 | 4 | 13,066 | 120 | 586,528 |

# A. Summary of Returns

## Scottish Funding Council Return

| Bursary Student Numbers & Expenditure | | | | | | |
|---|---|---|---|---|---|---|
| | Care Experienced | | Universal Credit | | Non-Maintenance | |
| | Students | £ | Students | £ | Students | £ |
| Maintenance Allowances: | 177 | 1,237,149 | 115 | 112,522 | - | - |
| Residence Costs | - | - | - | - | - | - |
| Dependents Allowance | - | - | - | - | - | - |
| Study Expenses Allowance | 54 | 5,789 | 36 | 7,241 | 117 | 15,650 |
| Travel Expenses Allowance | 18 | 9,976 | 65 | 43,642 | 8 | 3,171 |
| Additional Support Needs Allowance | - | - | - | - | 2 | 5,498 |
| **Total Numbers & Spend** | 178 | 1,252,923 | 115 | 163,405 | 124 | 24,319 |
| **Total Bursary Funds Spent in 2024/25** | | | | | | **2,817,538*** |

*Difference resultant from rounding.

# A. Summary of Returns

## Scottish Funding Council Return

| FE Discretionary Fund | Total Numbers & Spend | |
|---|---|---|
| | Students | £ |
| Students u18 | - | - |
| Parentally Supported (At Home) | 196 | 35,798 |
| Parentally Supported (Away from Home) | 3 | 3,166 |
| Self-Supporting | 107 | 117,877 |
| Care Experienced | 137 | 47,962 |
| Universal Credit | 76 | 22,816 |
| Non-Maintenance | 257 | 45,453 |
| **Total FE Discretionary Fund Spent in 2024/25** | **776** | **273,072*** |

*Difference resultant from rounding.

# A. Summary of Returns

**Scottish Funding Council Return**

| **Childcare Fund Expenditure** | | |
|---|---|---|
| | **Childcare Fund** | |
| | **Students** | **£** |
| At FE Level | 30 | 61,911 |
| At HE Level | 33 | 75,586 |
| **Total** | **63** | **137,497** |

**Auditors' Report**

We have examined the books and records of Forth Valley College and have obtained such explanations and carried out such tests as we considered necessary. On the basis of our examination and of the explanations given to us, we report that the information set out in these forms is in agreement with the underlying records. We also report that, in our opinion, the college used these funds in accordance with the Scottish Funding Council conditions. We are satisfied that the systems and controls of the administration and disbursement of these funds are adequate.

| | |
|---|---|
| Principal's Signature: | - |
| Auditors' Name: | - Wbg Services LLP |
| Auditors' Signature: | - Wbg Services LLP |
| Date of Signature: | - 3 October 2025 |

# A. Summary of Returns

## Student Awards Agency for Scotland (SAAS)

| HE Discretionary Fund | | |
|---|---|---|
| | HE Discretionary Fund<br>£ | Total<br>£ |
| **Income** | | |
| Total funds available for disbursement | 93,193 | 93,193 |
| **Expenditure** | | |
| Funds disbursed | 91,250 | 91,250 |
| **Remaining allocation from 2024/25; funds to be returned to SAAS by 31 October 2025** | **1,943** | **1,943** |

# A. Summary of Returns

## Students Award Agency for Scotland (SAAS)

**Auditors’ Report**
We have examined the books and records of Forth Valley College and have obtained such explanations and carried out such tests as we considered necessary. On the basis of our examination and of the explanations given to us, we report that the information set out above is in agreement with the underlying records and in our opinion is in accordance with the relative statutory requirements. We are satisfied that the systems and controls of the administration and disbursement of these funds are adequate.

Appointed Auditor: Wbg Services LLP Date: 3 October 2025

# B. Current Year Recommendations

**Manual Processing – Childcare Payments**

| Ref. | Finding and Risk | Grade | Recommendation |
|---|---|---|---|
| 1. | Childcare commitments are ordinarily managed via the Power BI suite to automate reporting and payment preparation.<br>During our review, we identified a duplicate payment of £14.25 to one student. A payment for two weeks was uploaded in error instead of a single-week payment when transactions were processed manually.<br>A temporary issue with the Power BI suite required manual uploads. Manual processing was not supported by equivalent controls to those embedded in the automated process.<br>There is the risk minor errors accumulate resulting in misstatement and overpayments to providers. | Low | We recommend that should core systems be unavailable, the College should establish additional checks on manual work to reduce the likelihood of recurrences. |

**Manual Processing – Childcare Payments**

| Management response | Responsibility and implementation date |
|---|---|
| Additional checks have been added to the process of manual commitments requiring to be uploaded, including a table of the payment weeks to automatically calculate the payments per fund, rather than this being completed entirely manually. | *Responsible Officer: Senga McKerr*<br>*Implementation Date: Immediate* |

# B. Current Year Recommendations

| Discretionary Payment Reconciliations | | | |
|---|---|---|---|
| **Ref.** | **Finding and Risk** | **Grade** | **Recommendation** |
| 2. | Discretionary payments to students are reviewed by the Senior Funding Officer, with periodic spot checks by the Systems & Management Accountant.<br>During our review, we identified an underpayment of £41 to one student. This was due to human error where the Finance Assistant had mis-keyed the payment run start date, resulting in the first payment to the student being missed. This was subsequently missed by the Senior Funding Officer and Systems & Management Accountant due to the low monetary value.<br>There is the risk an accumulation of minor errors may result in material misstatements. | **Low** | We recommend that the College look to establish an automated reconciliation between the approved award schedule and each payment run, with exception flags for missing first instalments or zero payments. |

| Discretionary Payment Reconciliations | |
|---|---|
| **Management response** | **Responsibility and implementation date** |
| We will look to add in some manual reconciliations between funds paid and funds committed (on a quarterly basis) which will help us to spot any errors like this in the future. There is not an automated solution for this situation. | *Responsible Officer: Senga McKerr*<br>*Implementation Date: 31 October 2025* |

# C. Grading Structure

For each recommendation we make we assign a grading either as High, Medium or Low priority depending upon the degree of risk assessed as outlined below:

| Grading | Risk | Classification |
|---|---|---|
| High | High Risk | Major weakness that we consider needs to be brought to the attention of the the Audit Committee and addressed by Senior Management of the College as a matter of urgency |
| Medium | Medium Risk | Significant issue or weakness which should be addressed by the College as soon as possible |
| Low | Low Risk | Minor issue or weakness reported where Management may wish to consider our recommendation |

# Forth Valley College

Internal Audit 2024/25

Education Maintenance Allowance

September 2025

# Table of Contents

# Disclaimer

*The matters raised in this report came to our attention during the course of our audit and are not necessarily a comprehensive statement of all weaknesses that exist or all improvements that might be made.*

*This report has been prepared solely for Forth Valley College's individual use and should not be quoted in whole or in part without prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any third party.*

*We emphasise that the responsibility for a sound system of internal control rests with management and work performed by internal audit should not be relied upon to identify all system weaknesses that may exist. Neither should internal audit be relied upon to identify all circumstances of fraud or irregularity should there be any although our audit procedures are designed so that any material irregularity has a reasonable probability of discovery. Even sound systems of control may not be proof against collusive fraud. Internal audit procedures are designed to focus on areas that are considered to be of greatest risk and significance.*

# 1. Executive Summary

### Introduction

This report has been prepared following the conclusion of our audit of the Educational Maintenance Allowance for the year ended 31 July 2025.

The audit certificate was submitted to the Scottish Funding Council (SFC) on 3 October 2025.

### Summary of Recommendations

| Current Year Recommendations | High | Medium | Low | Total |
|---|---|---|---|---|
| EMA Audit 2024/25 | - | - | 1 | 1 |

| Prior Year Recommendations | High | Medium | Low | Total |
|---|---|---|---|---|
| There were no recommendations made on the EMA Audit 2023/24. | | | | |

# 1. Executive Summary

### Conclusion

**Overall Conclusion:**

We have examined the books and records of Forth Valley College, including evidence of checks of 5% of applications and payments, with a sample size appropriate to the total number of applications, and have obtained such explanations and carried out such tests as we considered necessary.

On the basis of our examination and of the explanations given to us, we report that the information set out in these forms is in agreement with the underlying records.

We also report that, in our opinion, the College used these funds in accordance with the SFC's conditions and the principles of the Education Maintenance Allowance (EMA) programme.

We are satisfied that the systems and controls of the administration and disbursement of these funds are adequate.

## 2. Benchmarking

We include for your reference comparative benchmarking data of the number and ranking of recommendations made for audits of a similar nature in the year ending 31 July 2024.

| Benchmarking | High | Medium | Low | Total |
|---|---|---|---|---|
| Average no. recommendations in similar audits | - | - | 1 | 1 |
| Recommendations at Forth Valley College | - | - | 1 | 1 |

As can be seen from the above table, the College has a similar number of recommendations in comparison to the colleges it has been benchmarked against.

# 3. Audit Arrangements

We detail below our staff who undertook the review together with the College staff we spoke to during our review.

| **Wbg Services LLP** | | | |
|---|---|---|---|
| Partner | Graham Gillespie | Partner and Head of Internal Audit | gg@wbg.co.uk |
| Director | Stephen Pringle | Director of Internal Audit | sp@wbg.co.uk |
| Manager | Siobhan Archibald | Internal Audit Manager | sma@wbg.co.uk |
| Senior | Kyle McGuiness | Internal Audit Senior | kmg@wbg.co.uk |

| **Forth Valley College** | | | |
|---|---|---|---|
| Key Contact: | Allison Hewitt | Systems and Management Accountant | allison.hewitt@forthvalley.ac.uk |

Wbg appreciates the time provided by all the individuals involved in this review and would like to thank them for their assistance and co-operation. We can confirm that all data requested was ready on our arrival and the availability and assistance provided by the involved staff was greatly appreciated

# 3. Audit Arrangements

The table below details the dates of our fieldwork and the reporting of the audit area under review.

| Audit Stage | Date |
|---|---|
| Fieldwork start | 8 September 2025 |
| Closing meeting | 19 September 2025 |
| Draft report issued | 26 September 2025 |
| Receipt of management responses | 30 September 2025 |
| Final report issued | 1 October 2025 |
| Submission to Scottish Funding Council | 3 October 2025 |
| Audit Committee | 20 November 2025 |
| No of audit days | 3 |

# 4. Detailed Recommendations

| Spot Checks and Attendance Reports | | | |
|---|---|---|---|
| **Ref** | **Finding and Risk** | **Grade** | **Recommendation** |
| 1. | The College is required to complete spot checks on EMA applicants equivalent to 5% during the periods August 2024 to March 2025 and a further 5% between April and July 2025.<br>During our review, we identified five discrepancies in the spot-check process, all relating to attendance records. Further discussion and analysis confirmed that the College's systems generate varying attendance results depending on the timing and source of the data; this was verified during our site visit.<br>In addition, while the 5% spot-check requirement was achieved across both periods reviewed, we noted that in the April 2025 – July 2025 period the checks did not include new applicants.<br>There is the risk inaccurate spot checks may lead to overpayments and compliance issues. | Low | We recommend College systems are investigated to identify and resolve current inconsistencies. In the interim the College should develop clear guidance on where attendance records should be assessed.<br>We also recommend future spot checks during the second period are conducted on new applicants where possible. |

| Management Response | Responsibility and Implementation Date |
|---|---|
| We have re-written the processes for the EMA spot checks to include new awards for the second period in the sample selection, although this number is normally very low for College students (5 in 2024-25). The College's Business Transformation team is updating the attendance reports following issues we have had following the College switch to using PowerBI. | *Responsible Officer: Senga McKerr*<br>*Implementation date:  31 October 2025* |

# A. Audit Certificate

Name of College: Forth Valley College

Auditors’ Report to the Scottish Funding Council (SFC) for the period from 1 August 2024 to 31 July 2025.

We have examined the books and records of the above college, including evidence of checks of 5% of applications and payments, with a sample size appropriate to the total number of applications, and have obtained such explanations and carried out such tests as we considered necessary.

On the basis of our examination and of the explanations given to us, we report that (subject to the reservations set out in this report the information set out in these forms is in agreement with the underlying records.

We also report that, in our opinion, the College used these funds in accordance with the SFC’s conditions and the principles of the Education Maintenance Allowance (EMA) programme.

We are satisfied that the systems and controls of the administration and disbursement of these funds are adequate.

Signature: Wbg Services LLP

Name of Firm: Wbg Services LLP

Date: 3 October 2025

# B. Grading Structure

For each recommendation we make we assign a grading either as High, Medium or Low priority depending upon the degree of risk assessed as outlined below:

| Grading | Risk | Classification |
|---|---|---|
| High | High Risk | Major weakness that we consider needs to be brought to the attention of the the Audit Committee and addressed by Senior Management of the College as a matter of urgency |
| Medium | Medium Risk | Significant issue or weakness which should be addressed by the College as soon as possible |
| Low | Low Risk | Minor issue or weakness reported where management may wish to consider our recommendation |

# 9. Progress Report on Audit Recommendations
For Discussion

20 November 2025
AUDIT COMMITTEE

## 1. Purpose

**To update members on progress with the implementation of recommendations contained within internal and external audit reports.**

## 2. Recommendation

That members note the content of the report and associated appendix.

## 3. Background

The College monitors progress against internal and external audit recommendations and reports on progress to each meeting of the Audit Committee. This report provides assurance to the Committee that the College is appropriately managing all internal and external audit recommendations.

## 4. Summary of Changes

Recommendations contained within the reports presented to the September 2025 Committee meeting have been incorporated into the tracker. The attached annex contains an update on progress against recommendations.

Recommendation 1 has been progressed and we are awaiting feedback from JISC. This will necessitate a further revision to the completion date as shown in the annex.

In relation to recommendation id 11 – Sustainability Interim Targets, there have been no targets/framework set for the sector. As such the College is not in a position to set a completion date for this. The College will continue to report on progress against sustainability in the standard fashion, for example as part of the Annual Accounts.

Overall 5 of the 12 current recommendations have reached a stage where the college considers them to be completed. A summary of progress is below.

| | No Priority | Priority 1/ High | Priority 2/ Medium | Priority 3/ Low | Total |
|---|---|---|---|---|---|
| Live within date | 0 | 0 | 1 | 5 | 6 |
| Live recommendation passed implementation date | 0 | 0 | 0 | 1 | 1 |
| Completed since last report to Committee | 0 | 0 | 1 | 4 | 5 |
| Recommended for removal | 0 | 0 | 0 | 0 | 0 |

## 5. Resource Implications (Financial, People, Estates and Communications)

This is a summary report so there are no specific resource implications

## 6. Equalities

This is a summary report so there are no equalities implications

## 7. Communities and Partners

None

## 8. Risk and Impact

Please complete the risk table below. Risk is scored against Likelihood x Impact, with each category scored from Very Low through to Very High. Risks should be robustly scored and, if the combined score (Likelihood x Impact) is higher than the Board Risk appetite for the risk category identified, additional justification must be provided on why this risk is necessary.

If the paper is an approval, please reflect on whether the approval will have any direct or indirect impact for any other areas of operational activity internally or externally within the College – No

| | **Likelihood** | **Impact** |
|---|---|---|
| **Very High (5)** | | |
| **High (4)** | | |
| **Medium (3)** | | |
| **Low (2)** | X | X |
| **Very Low (1)** | | |

**Total Risk Score** – 4

The College has a Strategic Risk appetite for categories of risk as defined by the Board of Management. Decisions being taken at LMT/SMT/Board level must have cognisance of this. Please indicate the single most relevant risk category in the table below.

| **BoM Risk Categories & Risk Appetite (Select one area only)** | | | | | |
|---|---|---|---|---|---|
| **Cautious <15** | | **Open 15> <20** | | **Eager >20** | |
| Governance | X | Strategy | | People | |
| Legal | | Financial | | Project/Programme | |
| Property | | Reputational | | | |
| | | Technology | | | |

Audit recommendations continue to be actively managed by the College and are reported as a standing agenda item to the Audit Committee

**Is the score above the Board Risk Appetite level?** No

# 9. Progress Report on Audit Recommendations
For Discussion

20 November 2025
AUDIT COMMITTEE

| | |
|---|---|
| **Risk Owner –** Alison Stewart | **Action Owner –** Stephen Jarvie |
| **Paper Author –** Stephen Jarvie | **SMT Owner –** Alison Stewart |

| ID | Audit Name | Date of Audit | SMT Owner | Action Owner | Recommendation | Management Response | Priority | Evaluation | Scheduled Completion Date | Revised Completion Date | Evidence | Completed |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | IT Network Arrangements/Cyber Security | Nov-21 | Colin McMurray | Graeme Robertson | A risk-based approach should be adopted to enabling critical logs to improve endpoint security. Examples of critical logs include:<br>• Local user and group enumeration.<br>• Logon attempts with local accounts.<br>• Logon with explicit credentials.<br>• Plug-and-play device connections (e.g., USBs).<br>• Process creation.<br>• File creation.<br>• PowerShell providers loaded.<br>• Script block logging. | The College is currently on-boarding with Jisc to introduce a Security Information Events Management (SIEM) system, starting with logging at server level. It's planned to extend logging to key workstations once all parties are comfortable with how they system functions. This recommendation reflects where we are with our implementation. | 3 | Nov 2025 - Information provided to JANET and awaiting feedback<br>April 25 - Discussions are ongoing with Jisc due to the rising cost of their offering, with alternative solutions being explored.<br>November 24 - Jisc have re-engaged with on-boarding to their new offering, and revised pre-boarding paperwork and tasks have been completed by the College.<br>August 24 - Still engaging with Jisc, however no confirmed date for on-boarding.<br>April 24 - No change<br>November 23 - The College has continued to engage with preparations for entering a SIEM, and updated logs have been provided to Jisc, however there is no confirmed date for on boarding.<br>August 23 - No change at this time<br>May 23 - JISC have had to radically change it's SIEM offering, which put a stop to on boarding. They recommended on boarding early May with the new service but there is no indication at this time when the College will be able to do so. Other JISC recommended tools (pingcastle) have been used and action in response to | 31/08/2022 | 31/03/2026 | | |
| 2 | Credits Audit 23/24 | Sep-24 | Alison Stewart | Lesley Burn | We recommend the College ensures courses are correctly classified on the FES and ensures that credits are claimed for fundable students in line with the SFC guidance. | Prior to any future FES returns an additional check on HEI funded students will be undertaken to ensure that HEI funding is still the relevant recorded funding route. | Low | November 2025 - The audit of 2024/25 credits reconsidered this recommendation and stated "no further action required"<br>August 25 - No further update<br>Apr 25 - This will be actioned for the next FES return at the end of the academic year | 31/07/2025 | Oct-25 | 2024/25 credits audit report | Yes |
| 3 | Budgetary Control | May-23 | Alison Stewart | Senga McKerr | The College should develop realistic medium-term financial plans and forecasts to supplement the annual FFR and help to identify and mitigate emerging risks to its medium to long term financial sustainability. | The ability to develop sensible medium term plans depends on receiving 3-year funding allocations. SFC has acknowledged that Budget plus one further year is sufficient, and this is expected to be the FFR requirement in June. We will discuss with the Finance Committee members the level of forward planning they would like to see and we will look to develop these plans when we have additional clarity around key assumptions. | 3 | November 2025 - Recommendation reviewed. SFC have not provided the requisite longer term financial information to date so the recommendation cannot be progressed further.<br>August 2025 - No further update<br>Apr 25 - Following discussion at the November 24 meeting where removal had been recommended as per the comment below, it was agreed to keep this on the register. This now forms part of the wider College financial review so the end date has been removed. The Committee will be informed at the relevant time when the recommendation can said to be complete<br>November 24 - Due to the ongoing budgetary issues it is not possible to prepare medium term financial plans.<br>August 24 - No change<br>April 24 - with the late announcement of the indicative funding levels this year, it has not yet been possible to develop these plans and discuss them with the Board Committee. The college will take information to the Finance, Resource and Infrastructure Committee later this year<br>November 23 - discussion with FRAIC outstanding.<br>August 23 - To be discussed at Finance, Resource and Infrastructure committee in Sept 23. | 30/11/2023 | None | | |
| 4 | Corporate Governance | Apr-25 | N/A | Board Secretary | We recommend that the College establish a Development Plan for Board Members which will be subject for an annual review. | Agreed. A development plan will be put in place for the Board of Management. | Low | August 25 - Development plan will be presented for approval at the December Board meeting | Sep-25 | Dec-25 | | |
| 5 | Cyber Security | Jun-25 | Colin McMurray | Graeme Robertson | Cyber Security Risk Register - We recommend that the College establish a formal cyber or IT risk register to document and monitor key cyber security risks and vulnerabilities. This register should align with the format of the College's wider risk register, with risks assessed by likelihood and impact, assigned to owners, and reviewed regularly. | We agree that a formal I.T. cyber risk register be established, that is informed by standard procedures for checking particular sources for elements of risk to the college, coupled with horizon scanning for cyber risks should populate the risk register. This work has been carried out, and is part of the formal processes of the I.T. team. | Medium | | | | Cyber Risk Register | Yes |
| 6 | Cyber Security | Jun-25 | Colin McMurray | Graeme Robertson | Tabletop Exercises for Incident Management - We recommend that the College incorporates regular tabletop exercises to enhance the effectiveness of the IT Security Incident Response Plan already in place. The Incident Response Team should conduct exercises focused on security breach scenarios to reinforce the College's response capabilities. These exercises should include structured debrief sessions to capture lessons learned and refine the incident management framework. | We agree that the carrying out of table top exercises, should supplement the in-place incident response plan. The Cyber Incident Response Plan has been reviewed, and amended. The plans are for monthly table top incident response plan testing aligned with particular playbooks. On completion of all playbooks being tested, the tabletop exercises will be expanded to encompass work with other departments, and then work with the Learning Management Team (L.M.T.) | Medium | Nov 25 - planning for tabletops underway | Mar-26 | | | Yes |
| 7 | Cyber Security | Jun-25 | Colin McMurray | Graeme Robertson | Phishing Simulation Outcomes - We recommend that the College implement a more structured follow-up process for phishing simulation outcomes. This should include a requirement for line managers to confirm that they have discussed simulation failures with their staff and that any required training has been completed. For staff who repeatedly fall victim to phishing simulations, the College should consider targeted interventions, such as one-to-one guidance with the IT Team, to reinforce awareness and improve cyber hygiene. Establishing a process for tracking these follow-ups will help ensure accountability and allow the College to monitor progress over time. | We agree to improve the structure surrounding the phishing simulation campaigns, with the addition of a feedback loop as to responses from managers, of staff that have been caught/compromised. We will keep a record of staff/management with their responses, and feedback. | Low | | | | Record of feedback | Yes |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8 | Cyber Security | Jun-25 | Colin McMurray | Graeme Robertson | Data Leakage Prevention (DLP) - We recommend that a risk assessment which considers DLP is conducted to ensure that any areas of risk, such as the use of unmanaged USB storage devices, are assessed and that subsequent solutions are considered. The IT Team may then be tasked with providing additional security controls to mitigate these risks, helping the College to reduce the likelihood of deliberate or accidental data leakage. | We agree to strengthen the Data Loss Prevention (DLP) tools that we currently deploy, and will assess what that will entail. We will also explore other available tools within the Office 365 tenancy environment and see if they can help prevent DLP. | Low | Nov 25 - staffing assigned and review commenced | Apr-26 | | | |
| 9 | Cyber Security | Jun-25 | Colin McMurray | Graeme Robertson | Supply Chain Security - We recommend that the College establishes a mandatory requirement within procurement for relevant partners to evidence their cyber security credentials by providing copies of relevant certifications and recertifications when due. This will help provide ongoing assurance of current and future suppliers' cyber security standards. | We will explore this recommendation with the Procurement Team, with respect to the viability/practicality , given resource constraints. | Low | Nov 25 - currently in discussion with procurement manager | Apr-26 | | | |
| 10 | Sustainability & Carbon Management | Jun-25 | Alison Stewart | Martin Loy | Sustainability Reporting in the Annual Report and Financial Statements - We recommend that the College should integrate detailed emissions data, broken down by source and Scope 1, 2, and 3 and baseline comparisons from the Net Zero Plan into the Annual Report and Financial Statements. | Reasoned Recommendation; FVC to implement and provide information within annual report/financial statements as well as FVC annual Sustainability report. | Low | November 2025 - all necessary information has been provided for inclusion in the annual accounts which will be taken to the Board in December | Dec-25 | | Information in accounts | Yes |
| 11 | Sustainability & Carbon Management | Jun-25 | Alison Stewart | Martin Loy | Establishing Interim Targets - We recommend that the College develop and implement interim targets to support its 2040 net zero goal. These should include carbon reduction milestones for 2030 and 2035, as well as specific and measurable targets for water usage and waste reduction. Establishing these interim targets will create a clearer path toward the 2040 goal, support early identification of under performance. Progress against these targets should be reviewed and reported annually. | The College will set robust science-based targets to achieve Net Zero as an institution, once a sector-wide framework/methodology for this has been established.<br>It is crucial that the College's targets are both ambitious and realistic.<br>Currently frameworks such as the Science Based Targets Initiative only cover commercial businesses and not public bodies.<br>EAUC are working to produce a new framework which is specific to the sector and we will use this to produce Science Based Targets once this is available.<br>Until such a framework is published we will work towards the absolute targets provided by the Scottish Government (at the latest).<br>In the interim we will work towards a target of 42% reduction in baseline Net Zero Emissions by 2027/28 as laid out in FVC's Net Zero Plan 2023 -2027. | Low | November 2025 - Sector based targets/framework are not available at this time. | N/A | | | |
| 12 | Student Support | Jun-25 | Sarah Higgins | Sarah Tervit | Minuting Meetings - We recommend that all individual Teams, working groups and Management Team meetings are minuted with actions from the meeting being clearly noted. These minutes should be circulated to all those at the meeting to ensure that these are a true and fair record of what was discussed and agreed at the meetings. | Accept recommendation – as discussed during the audit period, this is an area that had already been identified for action for the forthcoming academic year, as part of the TQER process the college undertook in May 2025. | Low | November 2025 - Head of Information and Student Services conifrms that the recommendation was implemented and is now common practice for all meetings | Aug-25 | | Minutes of meetings | Yes |

# 10. Risk Management
# For Discussion

**20 November 2025**
**AUDIT COMMITTEE**

## 1. Purpose

**To present the current strategic risk register to members.**

## 2. Recommendation

That members consider the strategic risk register and comment on the content.

## 3. Background

The strategic risk register is presented at each meeting of the Audit Committee and annually to the Board so that members may review and comment on those risks deemed to be strategically important to the College.

The table below is a summary of the risk register. Individual risk documents are available in Admincontrol under Audit Committee/Strategic Risks/20 November 2025.

## 4. Changes to Strategic Risks

| Risk No | Date identified | Risk Title | Initial Risk Score | Last Residual Score | Current Residual Score | Movement in period | Risk Appetite Category | Risk Appetite Score | Risk Treatment | Board Committee | SMT Owner | Action Owner |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Apr-21 | Financial Sustainability | 25 | 25 | 25 | <-> | Financial | 20 | Accept with mitigation | FRAIC | DP COO | DP COO |
| 2 | Apr-21 | Estates Maintenance - affordability | 25 | 25 | 25 | <-> | Property | 15 | Accept with mitigation | FRAIC | DP COO | DP COO |
| 14 | Aug-25 | Three campus estate | 25 | 20 | 20 | ↓ | Reputational | 20 | Accept with mitigation | BOARD | DP COO | Principal |
| 15 | Aug-25 | Transformation Project | 25 | 20 | 20 | <-> | Reputational | 20 | Accept with mitigation | BOARD | DP COO | DP COO |
| 9 | Apr-21 | People Strategy delivery | 16 | 12 | 12 | <-> | People | 25 | Accept with mitigation | FRAIC | DP COO | HHR |
| 3 | Apr-21 | High quality learning experience | 20 | 15 | 8 | ↓ | Strategy | 20 | Accept with mitigation | LSE | VPLSE | VPLSE |
| 5 | Apr-21 | National Bargaining / Strike Action | 20 | 8 | 8 | <-> | People | 25 | Accept with mitigation | FRAIC | DP COO | DP COO |
| 6 | Apr-21 | Growing/influencing strategic partners | 12 | 12 | 8 | ↓ | Reputational | 20 | Accept with mitigation | BOARD | VPBI | VPBI |
| 8 | May-23 | Student Accommodation | 12 | 8 | 4 | ↓ | Financial | 20 | Accept with mitigation | FRAIC | VPBI | VPBI |
| 10 | Apr-21 | Major incident , eg campus closure | 16 | 8 | 8 | <-> | Strategy | 20 | Accept with mitigation | BOARD | Principal | DoO |
| 11 | May-22 | Malpractice | 12 | 8 | 8 | <-> | Reputational | 20 | Accept with mitigation | LSE | VPLSE | HQTE |
| 12 | Aug-24 | IT legacy equipment | 16 | 8 | 8 | <-> | Technology | 20 | Accept with mitigation | AUDIT | VPBI | VPBI |
| 13 | Sep-23 | Board Secretary arrangements | 6 | 3 | 3 | <-> | Governance | 15 | Accept with mitigation | BOARD | N/a | DP COO |

There have been four changes to the risk scores since the last report.

**Risk ID 14:** Score has been reduced to reflect the political pressure from Scottish Government to SFC to find a solution for the Alloa Campus.
**Risk ID 3:** Score has been reduced to reflect very positive outcome of the TQER.
**Risk ID 6:** Score has been reduced reflecting positive relationships with commercial companies and Scottish Government.

**Risk ID 8:** Score has been reduced following successful tender process and Board of Management approval.

## 5. Resource Implications (Financial, People, Estates and Communications)

The register itself does not require significant resource to manage however mitigating actions may require additional resource on a case by case basis.

## 6. Equalities

**Assessment in Place? – No**

The Risk Registers do not require equalities impact assessment. Individual risks may result in Equalities assessments being completed for new/revised College policies and procedures.

## 7. Communities and Partners - Not applicable

## 8. Risk and Impact

| | Likelihood | Impact |
|---|---|---|
| **Very High (5)** | | |
| **High (4)** | | |
| **Medium (3)** | | |
| **Low (2)** | X | X |
| **Very Low (1)** | | |

**Total Risk Score** – 4

The College has a Strategic Risk appetite for categories of risk as defined by the Board of Management. Decisions being taken at LMT/SMT/Board level must have cognisance of this. Please indicate the single most relevant risk category in the table below.

| BoM Risk Categories & Risk Appetite (Select one area only) | | | | | |
|---|---|---|---|---|---|
| **Cautious <15** | | **Open 15> <20** | | **Eager >20** | |
| Governance | | Strategy | X | People | |
| Legal | | Financial | | Project/Programme | |
| Property | | Reputational | | | |
| | | Technology | | | |

Risk continues to be comprehensively managed and reviewed, including comparing risk scores against the Board risk appetite levels, on an ongoing basis.

**Is the score above the Board Risk Appetite level?** No

**Risk Owner –** Kenny MacInnes
**Paper Author –** Alison Stewart

**Action Owner –** Kenny MacInnes
**SMT Owner –** Kenny MacInnes

## 11. Compliance Report For Discussion

20 November 2025
AUDIT COMMITTEE

### 1. Purpose

**To provide an overview of Complaints, Data Protection and Freedom of Information activity for academic year 2024/25.**

### 2. Recommendation

That members review and note the content of this report.

### 3. Background

The College has, among a wide range of legal responsibilities, specific responsibilities in relation to –

- Complaints
- Data Protection; and
- Freedom of Information

In order to provide assurance to the Board that the College is discharging these duties correctly, this report is prepared annually to the Audit Committee for member's consideration.

### 4. Key Considerations

4.1 Complaints

The information presented in this section of the report and anonymised in Appendix 1, covers the complaints received and responded to by the Executive Office and the Principal.

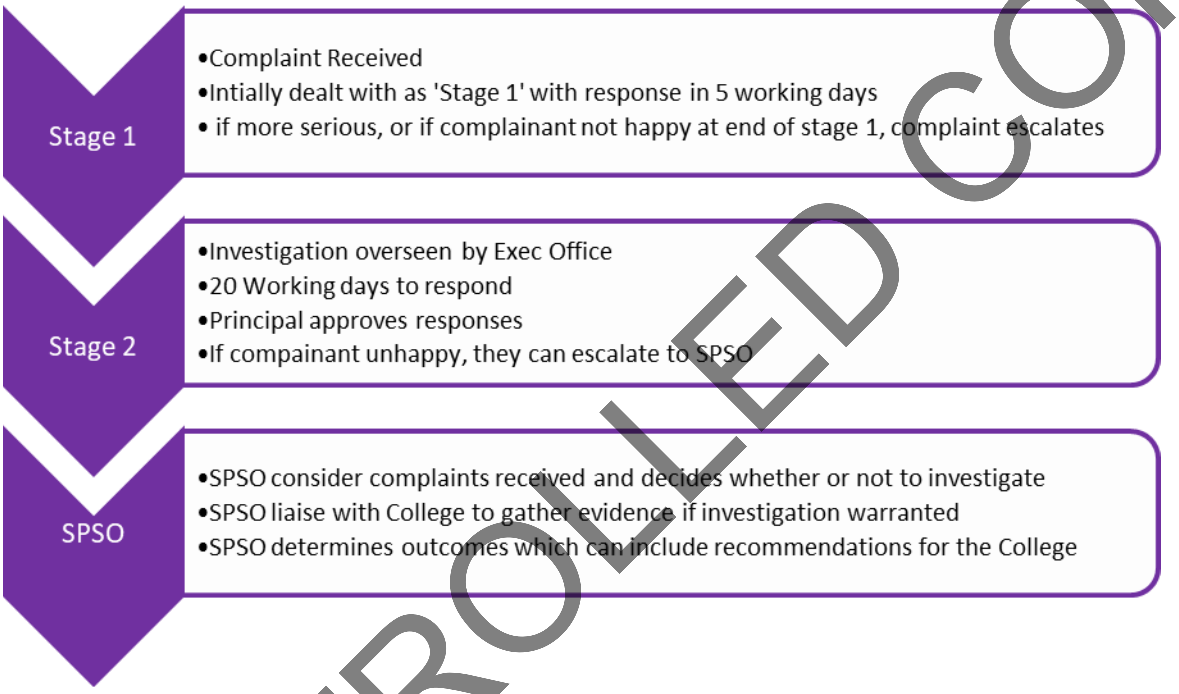
There are also lower level complaints which are dealt with routinely by operational staff and, in line with the College's complaints handling process as set out by the Scottish Public Sector Ombudsman (SPSO) in their Model Complaints Handling process which the College adopted to deal with complaints as close to the source of the complaint as possible.

36 matters were raised to the Executive Office in 24/25 as potential complaints. 24 were referred onto departments for dealing with at stage 1. 9 were dealt with by the Executive Office as stage 2 complaints. The Executive Office also provided support to those staff responding to the stage 1 complaints whenever requested.

3 matters received by the executive office were referred to other processes within the College that were more appropriate to the matter being raised (1x safeguarding, 1x allegation of student malpractice and 1x assessment related)

For fuller information on the College complaints handling process, please see - https://www.forthvalley.ac.uk/about-us/governance/complaints/

In brief, the complaints handling process is outlined below.



Stage 1

- Complaint Received
- Intially dealt with as 'Stage 1' with response in 5 working days
- if more serious, or if complainant not happy at end of stage 1, complaint escalates

Stage 2

- Investigation overseen by Exec Office
- 20 Working days to respond
- Principal approves responses
- If compainant unhappy, they can escalate to SPSO

SPSO

- SPSO consider complaints received and decides whether or not to investigate
- SPSO liaise with College to gather evidence if investigation warranted
- SPSO determines outcomes which can include recommendations for the College

4.1.1 Changes to the SPSO complaints system

Following the implementation by Scottish Government of the "United Nation Convention on the Rights of Children (UNCRC) (Incorporation)(Scotland) Act 2024", the legal definition of a child in Scotland changed to anyone under the age of 18 as of 16 July 2024.

In reflection to this, SPSO has developed new guidance to be utilised and is anticipating all organisations to be compliant within the 18-24 months of its launch.

The College has reviewed its complaint handling processes and has commenced the following actions which should be fully implemented in 2025/26.

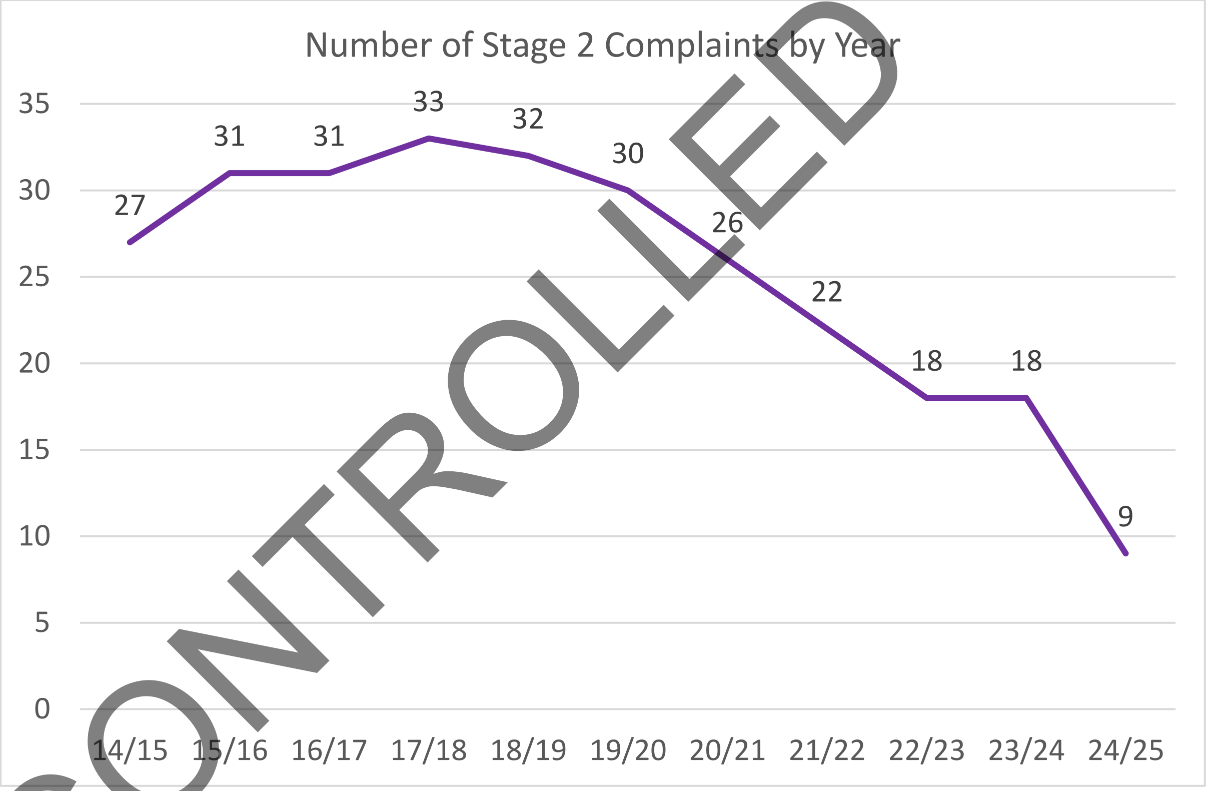
- Increased the number of staff involved in complaint handling. The Corporate Governance and Planning Officer will now be responsible for corporate related complaints, and the Quality and Teaching Enhancement team will be responsible for all teaching and learning related complaints.
- Supported by JISC, the College is seeking to develop an existing system, Unidesk, to administer all complaint activity within the College. This will bring a series of improvements including comprehensive tracking of stage 1 complaints, the ability

to ensure all complaints are being processed to SPSO timelines, identification of any trends in complaints at lower levels; and ensuring the child friendly approaches are being fully implemented.

- A number of College staff will be undertaking SPSO training on the child friendly complaints process.

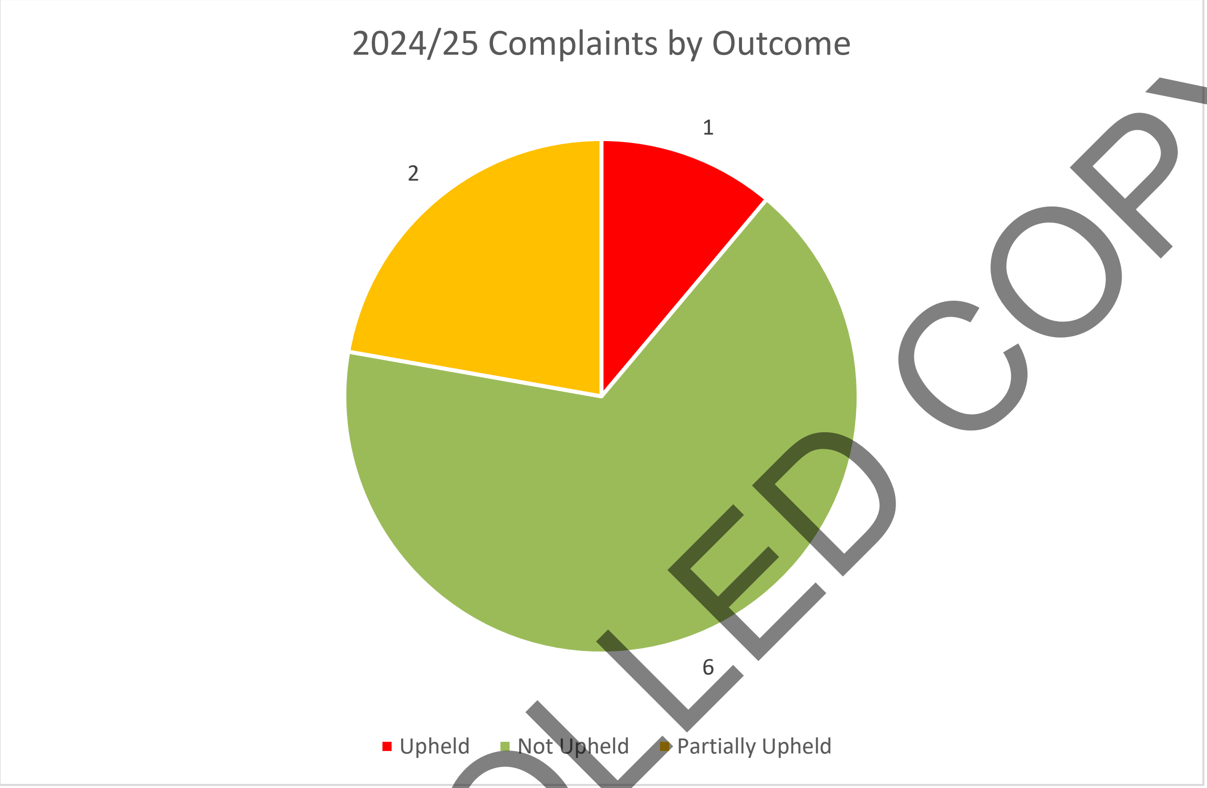
4.1.2 Complaints received in academic year 2024/25

The number of stage 2 complaints at Executive Office level has dropped compared to previous years.



In 2023/24 there were a significant number of complaints (11 out of 18 or 61%) of complaints alleged against staff. Of those complaints, 3 were upheld, 1 partially upheld and the other 7 were not upheld).

In 2024/25, the number of complaints relating to staff was reduced as a proportion of total complaints (44%) but was still the highest single group of complaints. Of the 4 complaints relating to staff, 1 was partially upheld and 3 were not upheld after investigation)



What the data outlined in the preceding charts do not show however, is the continued complexity of complaints.

At a sector level, comparing the total number of complaints received against data published by other College's demonstrates the College is slightly lower than a typical number of complaints.

4.2 Data Protection

4.2.1 Data Breaches

The College has a process in place for the recording, and if necessary, investigation of potential data breaches.

The team consisted of the Vice Principal Infrastructure and Communications, the Corporate Governance and Planning Officer; and the College Data Protection Officer (DPO). For info the DPO is an externally provided service.

Upon notification of a breach or potential breach, this group and any other relevant staff will assess the breach and whether or not it is notifiable to the Information Commissioners Office (ICO) and the subjects of a breach.

There were 4 reported data incidents in 2024/25 down from 9 in 2023/24. There was no significant trend given the low numbers and Appendix 2 provides further detail on each incident.

Comparator data with other Colleges in the sector is not available.

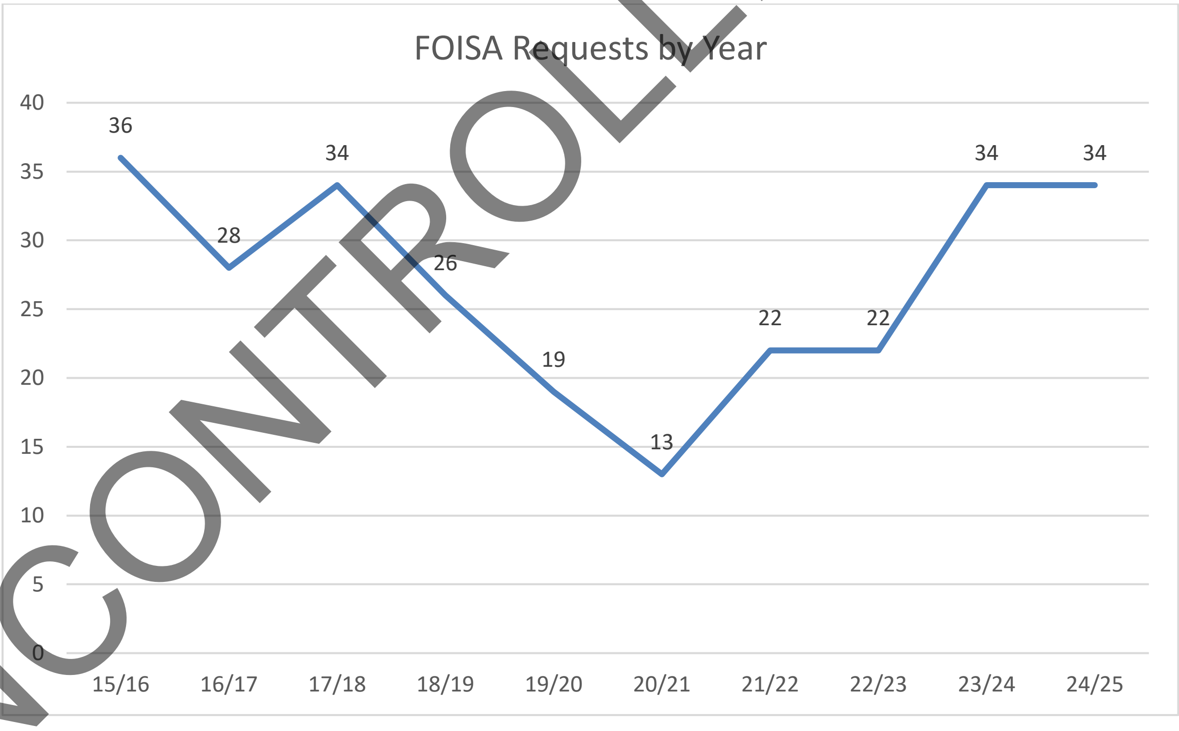
4.2.2 Subject Access Requests

There was one request under the right to be forgotten aspect of the legislation.

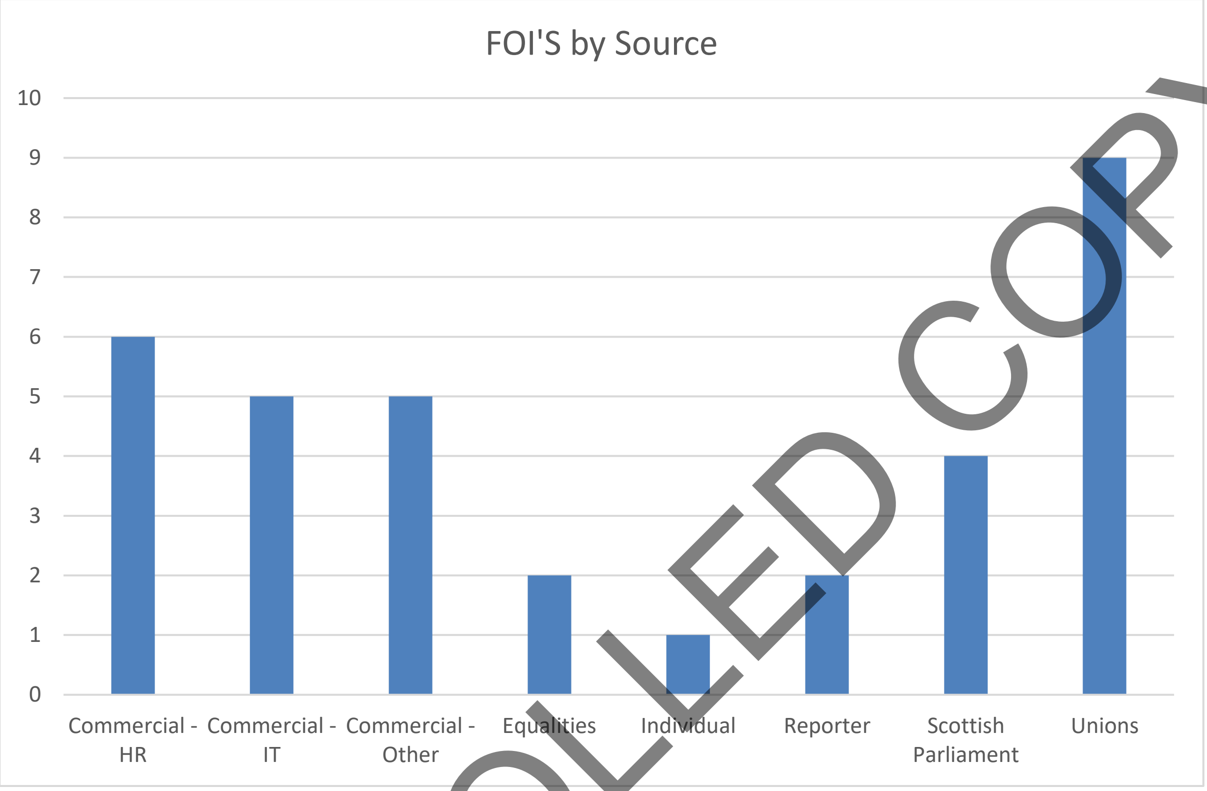
This request were actioned within the required timescales.

## 4.3 Freedom of Information (Scotland) Act 2002 (FOISA) Requests

There continues to be a high level of demand under FOISA, with 34 requests again this year.



In terms of sources of requests, this remains mixed as per previous years. This is around average for the sector.



When comparing the College FOI activity to the sector average (as per the table below) we can see that the number of FOIs is roughly in line with the sector indicating there has not been any particular FOI focus on the College. The figures differ slightly from those reported above owing to slightly different reporting periods.

Sector wide, approximately 90% of requests have received a response within the relevant timescale whereas the College responded to 97% within timescale, with one response being 3 days late.

In relation to the type of requests, there was a wide disparity in requests ranging from procurement related to equalities. Further information is contained in Appendix 3.

There were no clear trends other than a rise in queries relating to union membership across the various unions with staff in the College.

## 5. Resource Implications (Financial, People, Estates and Communications)

As noted earlier, meeting our differing requirements under the three areas reported on can have a significant impact on staff time and planning, especially where complaints are concerned.

## 6. Equalities

There are no impacts associated with this paper. Equalities issues that may be identified will always be addressed at the time.

## 7. Communities and Partners

None

## 8. Risk and Impact

Please complete the risk table below. Risk is scored against Likelihood x Impact, with each category scored from Very Low through to Very High. Risks should be robustly scored and, if the combined score (Likelihood x Impact) is higher than the Board Risk appetite for the risk category identified, additional justification must be provided on why this risk is necessary.

If the paper is an approval, please reflect on whether the approval will have any direct or indirect impact for any other areas of operational activity internally or externally within the College – No

| | **Likelihood** | **Impact** |
|---|---|---|
| **Very High (5)** | | |
| **High (4)** | | |
| **Medium (3)** | | **X** |
| **Low (2)** | **X** | |
| **Very Low (1)** | | |

**Total Risk Score** – 6

The College has a Strategic Risk appetite for categories of risk as defined by the Board of Management. Decisions being taken at LMT/SMT/Board level must have cognisance of this. Please indicate the single most relevant risk category in the table below.

| BoM Risk Categories & Risk Appetite (Select one area only) | | | | | |
|---|---|---|---|---|---|
| Cautious <15 | | Open 15> <20 | | Eager >20 | |
| Governance | X | Strategy | | People | |
| Legal | | Financial | | Project/Programme | |
| Property | | Reputational | | | |
| | | Technology | | | |

Failure to meet our regulatory requirements in relation to complaints, Data Protection or FOI can open the College up to reputational and legal consequences.

The College mitigates these risks by actively management of the processes by the Executive Office with oversight and sign off on all matters from the Principal or relevant SMT member.

**Is the score above the Board Risk Appetite level?** No

**Risk Owner –** Kenny MacInnes **Action Owner –** Stephen Jarvie

**Paper Author –** Stephen Jarvie **SMT Owner –** Kenny MacInnes

**Appendix 1**

**Complaints overview**

| ID | Type | Complaint | Investigation Outcome | Complaint Upheld? | Action Taken | Lessons Learned/ Notes |
|---|---|---|---|---|---|---|
| 1 | Staff Conduct | Follow up from complaint in June 2024 in regard to a staff member. The complainant was requesting information on the outcome of the disciplinary action taken. | The information in the original, upheld, complaint response was reiterated in that, things had moved forward via HR but that this could not be commented on further owing to data protection implications | No | None | None |
| 2 | Assault | The mother of a student physically assaulted on campus, but a group of external individuals complained that College staff had been too slow to intervene, should have been aware that there were a group of non-College teenagers on campus and there was delays contacting the police | An investigation was undertaken by a senior member of staff that had not been involved in the incident. No staff were in line of site of the initial attack or heard the commotion. On being informed of the assault, a manager, three facilities assistants went to stop the fight. | Partially | A college working group has been established to look at security on campus as well as behaviours in classrooms | While the incident was over and the student being cared for by a College first aider, 999 is still a more appropriate route in response to the level of violence. This has been reinforced with staff involved |

| ID | Type | Complaint | Investigation Outcome | Complaint Upheld? | Action Taken | Lessons Learned/ Notes |
|---|---|---|---|---|---|---|
| | | | With the College being a public building and the group being of age with a majority of students, it was not reasonable to conclude front of house staff should have known these were not students or were here with ill intent. It was acknowledged that, once the incident was broken up and the perpetrators escorted from campus, staff initially tried to call police on 101 and should have dialled 999 instead | | | |
| 3 | Staff Conduct | A former member of staff complained, alleging that senior staff within their department had divulged personal information in relation to them | All claims within the complaint were investigated, staff interviewed, and the allegations were unable to be substantiated | No | None | None |

| ID | Type | Complaint | Investigation Outcome | Complaint Upheld? | Action Taken | Lessons Learned/ Notes |
|---|---|---|---|---|---|---|
| 4 | Application | A student complained that their curriculum manager had made an unfair decision in not allowing them to progress to the next level of their course | The investigation showed poor attendance, lack of achievement and lack of engagement with staff from the department when they tried to help catch the student up | No | None | None |
| 5 | Course Delivery | A student complained that their evening course was poorly delivered, there had been poor communication from the College about the arrangements for the course; and that students did not feel supported. | The investigation showed that there had been underlying staff availability issues that impacted on the class. | Yes | The Principal apologised for the experience of the students. The Department were instructed to develop and deliver individual learning plans for each student on the course to help them achieve. | While the College has limited control over staff absence etc, there should have been better communication with the class and monitoring of progress |

| ID | Type | Complaint | Investigation Outcome | Complaint Upheld? | Action Taken | Lessons Learned/ Notes |
|---|---|---|---|---|---|---|
| 6 | Work Placement | A parent complained about the distance to the work placement their child had to travel via public transport | The investigation demonstrated that the student had been provided with some placement options and the one the parent was unhappy about was the one the student had chosen themselves | No | None | None |
| 7 | Staff conduct | A student raised a range of concerns regarding the conduct of their lecturer | This complaint took longer than normal to complete as the student missed multiple meetings with senior College staff to talk through the issues. The underlying cause was eventually identified as the student had concerns about not passing their course and was trying without foundation to blame staff | No | A support plan was developed and put in place to assist the student on catching up on missed work with a view to achieving their qualification | None |

| ID | Type | Complaint | Investigation Outcome | Complaint Upheld? | Action Taken | Lessons Learned/ Notes |
|---|---|---|---|---|---|---|
| 8 | Student Conduct | A local resident complained about student parking in the streets surrounding one of our campuses. This resident has raised similar issues in the past. | The evidence provided with the complaint showed that the cars were not on College grounds and appeared to be legally parked. | No | Complainant was again informed that the College has no authority over students parking legally on public roads. The College did re-issue guidance to the campus about being mindful of the local community | None |
| 9 | Staff Conduct | A grandparent complained about interactions between a staff member and the student in relation to a disciplinary matter and that the College did not take the students ASN into consideration | An investigation showed that neither the student nor the school they progressed from had informed the College of any ASN requirements, however it was acknowledged that the College was generally aware of this issue with schools transition so | Partially | The need for effective transitions information for students with ASN coming from schools has been the subject of an ongoing project and this | The need to improve transitions arrangements |

| ID | Type | Complaint | Investigation Outcome | Complaint Upheld? | Action Taken | Lessons Learned/ Notes |
|---|---|---|---|---|---|---|
| | | | partially upheld this part of the complaint. The disciplinary related matters were, at the time of the complaint, progressing under the appeals process under disciplinary so could not be considered as a complaint owing to SPSO guidance. In relation to comments made by staff, it was not possible to make a determination | | complaint was fed into the team | |

**Appendix 2 Data Incidents**

| ID | Type | Incident | Impact | Reportable to ICO? | Action Taken | Lessons Learned |
|---|---|---|---|---|---|---|
| 1 | College System | While demonstrating the new HR system to a member of staff, their manager logged in as themselves owing to access rights to show some of the functionality and inadvertently put personal health related on display | Low – There was a quick response by the manager to scroll away from the information and it is unknown whether the other staff member present noticed the relevant detail | No | Requested that all system demonstrations in relation to HR use test data only | The need to ensure test data is used |
| 2 | Email | A member of staff sent an email to 15 students with their email addresses in the CC rather than BCC fields. This was the result of human error | Low – there was no other information than the email addresses | No | Corporate Governance officer spoke to the staff member and their manager | Email continues to be an area of concern |
| 3 | Teams | Two teams' areas had been created to collate documentation for the quality audit in early 2025. This information contained the outputs from 'Listening to learners' sessions. The areas had been mistakenly set as public rather than private and the issue was raised by a student | Low – a comprehensive review of access logs for the areas showed the student had only accessed the top level of the team and not the listening to learner's content. The logs also | No | Teams areas set immediately to private. Team counselled on the appropriate security arrangements | To remember that public teams are available to all on the College teams system |

| ID | Type | Incident | Impact | Reportable to ICO? | Action Taken | Lessons Learned |
|---|---|---|---|---|---|---|
| | | | showed no other concerning access | | | |
| 4 | Assessment | A completed assessment document by one student was shared accidentally with another class via Teams | Low – the only personal information was the students name, and the content of the assessment was not in relation to their private life | No | Staff counselled | To verify the correct attachment is being sent to students |

**Appendix 3 – Freedom of Information Requests**

| ID | Origin of Request Type | Regarding | Response (Full/Partial/None) |
|---|---|---|---|
| 1 | Commercial – HR | Curriculum manager role description | Full |
| 2 | Reporter | VA and Compulsory Redundancies | Full |
| 3 | Scottish Parliament | Trade Union Facility Time costs | Full |
| 4 | Commercial – HR | Recruitment spend | Full |
| 5 | Commercial – HR | Employee engagement spend | Full |
| 6 | Commercial – IT | Software information | Full |
| 7 | Commercial – HR | Staff survey information | Full |
| 8 | Unions | Support staff pay award | Full |
| 9 | Commercial – Other | Confidential waste services | Full |

| | | | |
|---|---|---|---|
| 10 | Commercial – Other | Fair trade spend | Full |
| 11 | Unions | 30 Years of Principal Salary Information | Partial – some information not held |
| 12 | Unions | Fire Arrangements for Deaf Staff | Full |
| 13 | Unions | ASN course cuts over last 5 years | Full |
| 14 | Commercial - Other | Water and waste services | Full |
| 15 | Commercial - IT | HR and finance software systems | Full |
| 16 | Unions | Number of staff paying union fees via payroll deduction | Full |
| 17 | Equalities | Communications support | Full |
| 18 | Individual | Plumbing course completion information | Full |
| 19 | Commercial - IT | Network infrastructure | Full |
| 20 | Unions | Number of awards received by the College in the last 10 years | Full |
| 21 | Scottish Parliament | Salary band information | Full |
| 22 | Commercial - IT | Numbers of IT equipment | Full |
| 23 | Commercial - Other | Facilities Management information | Full |
| 24 | Unions | Number of staff paying Unison dues via payroll | Full |
| 25 | Scottish Parliament | Information on college legal team and external legal costs | Full |
| 26 | Unions | Information relating to pay | Full |
| 27 | Scottish Parliament | Budget and staff information | Full |
| 28 | Commercial - IT | IT and Cybersecurity services | Full |
| 29 | Commercial - Other | Finance/HR information | Full |
| 30 | Equalities | Freedom of speech practices | Full |
| 31 | Reporter | Student numbers | Full |

| | | | |
|---|---|---|---|
| 32 | Commercial - HR | Non-academic temp staff spend | Full |
| 33 | Unions | Spend with Israeli linked organisations | Full |
| 34 | Commercial - HR | Graphic design services | Full |

## Forth Valley College

### 14. Forward Agenda

| | May-26 | Sep-26 | Nov-26 |
|---|---|---|---|
| Apologies, Declaration of Interests and Changes to Members' Register of Interest | ✓ | ✓ | ✓ |
| | | | |
| **FOR APPROVAL** | | | |
| | | | |
| Minutes and Matters Arising | ✓ | ✓ | ✓ |
| Review of Action Tracker | ✓ | ✓ | ✓ |
| Review of Committee Remit | | ✓ | |
| Annual Report and Financial Statements | | | ✓ |
| External Audit Annual Report to the Board of Management | | | ✓ |
| Response to letter to those charged with governance | | | ✓ |
| Audit Needs Assessment | | ✓ | |
| Governance Statement | | ✓ | |
| Audit Committee Self-Assessment | | ✓ | |
| College Data Policy | ✓ | | |
| Risk Management | ✓ | | |
| | | | |
| **FOR DISCUSSION** | | | |
| | | | |
| Presentation of Internal Audit Reports | ✓ | ✓ | ✓ |
| - Safeguarding, Wellbeing and Counselling | ✓ | | |
| - Health and Safety | ✓ | | |
| - Change Management Phase 1 | ✓ | | |
| - Business Continuity & Disaster Recovery | | ✓ | |
| - Follow Up Review | | ✓ | |
| - Change Management Phase 2 | | ✓ | |
| Progress Report on Audit Recommendations | ✓ | ✓ | ✓ |
| Risk Management | ✓ | ✓ | ✓ |
| Internal Audit Annual Report | | ✓ | |
| Compliance Report (Complaints, FOI, Data Protection) | | | ✓ |
| | | | |
| **FOR INFORMATION** | | | |
| | | | |
| Forward Programme of Committee Business | ✓ | ✓ | ✓ |
| | | | |