Dumfries and Galloway College
One step ahead

Status: Approved

FINANCE AND GENERAL-PURPOSE COMMITTEE

MINUTE OF MEETING HELD ON 13 SEPTEMBER 2023 AT 16:00 VIA TEAMS

Present:		
Richard Nash (Chair)	Joanna Campbell (JC)	Claire McLean (CM)
Caroline Stuart (CS)	Jamie Ross	Susan McLellan (SM)
In attendance:		
Karen Hunter (KH)	Douglas Dickson (DD)	Joe McGraw (JM)
Alexandra Elkins (note taker)		
Apologies:		
Kate Glendye (KG)	Bill McMillan (BM)	Lorraine Grierson (LG)
Eddie Black (EB)		

1. Welcome and Apologies for Absence | Verbal | Chair R Nash

1.1.1. The Chair welcomed everyone to the meeting and the meeting was recorded as quorate.

1.1.2. Apologies were noted as shown above.

1.2. Declaration of Interests and Connections | Verbal | Chair R Nash

1.2.1. The Chair reminded Members to indicate any declaration of interest or connections as appropriate throughout the course of the meeting. C. McLean declared an interest in the appointment of the Vice Principal People and Transformation.

FOR APPROVAL

2. Minutes of Previous Meetings and Matters Arising

2.1. Minute of Meeting held 08 June 2023 | Paper 2.1 | Chair R Nash

2.1.1. The minutes were approved as an accurate record of the meeting.

2.2. Action Log | Paper 2.2 | J. Campbell

2.2.1. The Committee noted that one action remained open and the Condition Survey Report would be tabled at the next F&GP meeting in November 2023.

2.2.2. **The Committee noted the update to the Action Log.**

3. Item 3 - Strategic Risk Register | Paper 3 | J. Campbell

3.1. Following review by the Executive Leadership Team there had been no change to the scoring or mitigations for Risks 3 & 7, which sit with the FGP Committee.

3.2. The HR Sub-Committee had discussed both risks and proposed that they are unchanged.

3.3. One Member raised concern that the narrative of Risk 7 did not accurately reflect local Trade Union relations or the wider scope of effective industrial relations, which is more than strike action. …

3.4. **Agreement was reached that the wording of Risk 7 be revised**.

3.5. …

3.6. It was confirmed that five business cases identified with F&GP, relating to Risk 3 - Institutional Sustainability would be brought to and reviewed at the next Board of Management meeting.

3.7. The F&GP queried the rating of the likelihood of Risk 3 and the Executive's confidence in the budget. The Principal was confident that the forecast would be met and it was agreed that the scoring for Risk 7 remain unchanged.

3.8. **The Committee approved the risk register.**

4. Item 4 - Finance, Strategy & Sustainability | K Hunter

4.1. Management Accounts – Year end Position | Paper 4.1 | Approval | K Hunter

4.1.1. KH introduced the Draft Outturn for AY 22/23 and assumptions, included assumptions for the pension scheme. The July 2023 outturn was subject to Audit, and a small surplus was shown. The SFC had agreed clawback for AY2021/22 which had resulted in no change. Pay awards for 2022/23 were based on the current offer and any change would need to be reflected prior to final submission. Both the pay award and clawback remained unpaid at the time of the meeting which was reflected in the accounts.

4.1.2. F&GP noted key changes including ring-fenced funds for Mental Health and Counsellors, the Pathfinders Project, and Young Persons Guarantee funding as well as estimated SFC income and pay costs for the Job Evaluation project.

4.1.3. The F&GP requested information of any bad debts over £1000 and it was confirmed that no bad debts were reported at year end over £1000.

4.1.4. The Chair advised the Executive of the potential to generate income from the use of overnight deposits from the bank balance … (pending balances and banking arrangements). It was agreed to explore arrangements for overnight deposits.

4.1.5. ACTION: KH to research overnight deposits and discuss arrangements with RN.

4.1.6. Pension Valuation

4.1.7. The external auditors had requested scrutiny of the pension assumptions which would be included in the year-end statements. The Committee was asked to provide feedback on the assumptions.

4.1.8. The Chair reminded the Committee of their role to ensure appropriate assumptions are used based on actuarial advice. The F&GP discussed the assumptions including salary

growth which were based on triennial valuations and noted that any movement in the valuation of the pension fund would impact on the annual accounts.

4.1.9. The F&GP recommended a 'stress test' to show a realistic asset, reflecting more up-to-date salary growth and inflation expectations. The F&GP committee rejected the initial assumptions on the basis of its overly optimistic surplus valuation and new assumptions applied.

4.1.10. The F&GP scrutinised several items which were beyond the budget assumptions as well as the request for additional working capital. Further detail was provided.

4.1.11. The F&GP requested that the accounts be presented with additional commentary of any variances above a 5 or 10% tolerance. The Committee agreed with the approach.

4.1.12. ACTION: KH to update pension valuation assumptions more in keeping with current market conditions.

4.1.13. ACTION: KH to provide revised monthly management accounts with agreed amendments for approval.

4.2. **Contribution Report | Paper 4 | K Hunter**

4.3. The new Contribution Report was introduced based on the 23/24 budget with further refinement anticipated. The F&GP was asked to provide feedback on the format.

4.4. The F&GP commended the report and welcomed the information which would assist with more analysing financial performance of course offerings. The Committee advised caution with overcomplicating the report and to ensure that data aligns with the budget and monthly management accounts to provide confidence.

4.5. The F&GP were advised that the report was based on the student database and further improvements in some coding errors and reporting was expected. The executive advised caution on any reactive decision making based on the report and provided detail on the additional measures deployed to support decision making for both commercial and curriculum delivery.

4.6. The Principal explained several improvements and challenges in reporting and highlighted the requirement to achieve the College's credit target. More flexible funding approaches were being explored with the SFC.

4.7. …

4.8. **The Committee approved the contribution report.**

5. Terms of Reference / Self Evaluation | Paper 5.1 | L Grierson

5.1. The outcome of the F&GP Committee self-evaluation had been circulated and approved in advance of the meeting.

5.2. The Committee were advised of 2 changes.

- C.7 (D) of the quorum for the Committee to be set at 50% or higher ensuring that the majority in any decision making are non-executive members.

- The Terms of Reference now include the Committee Schedule of Business for each meeting.

5.3 A discrepancy on page 3, item 1.1 *'Minimum of 3 non-executive board members'* was highlighted. It was agreed that it be changed from 3 to 4 to reflect the agreed quorum.

5.4 A query of the name *'Finance and Performance Strategy'* was raised on item 4.1.9, and it was agreed that this would be checked.

5.5 ACTION: KH to check the name at item 4.1.9 and report back.

5.6 ACTION: Item 1.1 to be changed to reflect agreed quorum.

5.7 **The Committee approved changes to the Terms of Reference with agreed actions.**

FOR DISCUSSION

6. Learning, Skills & Student Experience

6.1. **… Confidential to members only.**

6.1.1. **The Committee noted the paper.**

6.2. **Commercial Business Case (approval) | Paper 6.2 | D. Dickson**

6.2.1. … **Confidential to members only**

7. People & Transformation

7.1. **HR Sub Committee Update (progress towards KPIs) | Verbal | C. McLean**

7.1.1. A verbal summary of the first HR Sub-committee meeting was provided which would allow sufficient scrutiny of HR matters and report to the F&GP.

7.1.2. The Committee welcomed the introduction of the workforce framework and it was noted that despite a variety of challenges experienced within the HR team over the past 12 months, the recent audit had provided reasonable assurance.

7.1.3. **The F&GP noted the verbal update.**

7.2. **Information Governance Update (Data Protection Compliance /FOI / Digital Services) | Paper 7.2 | J McGraw**

7.3. The F&GP noted 5 FOI requests and the Data Protection and Digital Information Bill was now at Public Bill Committee report stage. Privacy notices had been updated, and one minor GDPR incident was reported. The Cyber Action Plan was tabled for discussion at the next Audit Committee meeting.

7.4. **…**

7.4.1. **The Committee noted the update.**

7.5. **ICT Security Policy and ICT Acceptable Use Policy (approve changes) | Paper 7.3 | J**

McGraw

7.6. As part of the review cycle the policy had been reviewed and now included guidance on the use of USB drives.

7.7. The Chair advised caution on the use of USB drives.

7.8. One Member raised a concern about the methods by which staff provide feedback to students. The Committee was assured that awarding body procedures and assessment policy as well as internal quality processes, staff training and GTCS standards all contributed to very low reporting of incidents.

7.9. The F&GP also highlighted communications and briefings and queried methods to deliver information to staff face to face. A comprehensive list of the variety of platforms and regular meetings was shared and it was stated that in some areas communication by email was being discouraged with a move towards 'chat' options. The Principal added that regular meetings were also held with student representatives and the size of the College enabled a variety of all staff events throughout the year.

7.10. **It was suggested to add a bullet point on page 18 of the Appendix to prohibit the use of IT equipment for any illegal activities. This was agreed.**

7.11. **ACTION: JMc will instruct the IT Manager to amend the appendix as agreed.**

7.3.3 **The Committee noted the Policy and approved the changes with agreed actions.**

8. AOCB

8.1. There was no other business. The meeting was adjourned at 18:01 hours.

9. Date of the Next Meeting

9.1. The date of the next meeting is scheduled for Wednesday 15 November 2023.

Dumfries and Galloway College
One step ahead

Key
- Ongoing
- Closed
- Overdue

F&GP COMMITTEE ACTION LOG 13.09.23

No	Meeting Date	Action	Lead	Deadline	Status	Commentary
1	7/3/23 8/6/23	The Committee requested that a contribution report to understand the profitability of each course, be provided to the Committee for the next academic session. Contribution Report to be itemised in the September meeting agenda	KH LG	Sep 23	Closed	This has been tabled for the meeting scheduled 13/9/23.
2	7/3/23	Increased trend in staff absence – JG suggested the inclusion of a KPI style dashboard for absence reporting.	JM	~~May 23~~ Sep 23	Closed (moved to HR Sub Comm)	This item has been moved to the HR Sub-Committee Action Log and referred to the new VP People for consideration and action.
3	8/6/23	The Secretary to the Board will amend Risk 7 as agreed	LG	Sep 23	Closed	Risk 7 net likelihood has been increased from 4 to 5
4	8/6/23	KH to provide additional detail on supplies and service costs and marketing costs.	KH	Sep 23	Closed	Sent to FGP Members on 11 July 2023.
5	8/6/23	Narrative from SFC re parameters for setting the draft budget to be sent to members.	LG/KH	Sep 23	Closed	Annex A from SFC sent to FGP members on 11 July 2023.

No	Meeting Date	Action	Lead	Deadline	Status	Commentary
6	8/6/23	Business cases, as outlined in the budget report, to be developed and included as standing items.	Exec Team	Oct 23	Closed	Business cases will be included in the Performance Report to BoM for each BoM meeting. UWS Summary update will be a standing item on BoM agenda.
7	8/6/23	Commercial 8a) Business Case for capital investment and market demand to be submitted to the Committee for approval. 8b) The Committee requested comparative data for all marketing performance stats (previous year) to be provided in future reports	BM	Sep 23	Closed	Business case to be submitted at the FGP meeting scheduled for Sep 23. Comparative data to be included where available and incorporated moving forward.
8	8/6/23	Condition Survey Report A detailed report with 5-year plan to be presented to the Committee.	BC	~~Sep 23~~ Nov 23	Ongoing	This has been moved to the next FGP meeting alongside the Estates Annual Report.

MEETING	FINANCE AND GENERAL PURPOSES COMMITTEE
AGENDA ITEM:	**3**
PAPER NO:	**FGP-0623-3.1**

Date	08 June 2023
Location	MS Teams On-line
Title of Paper	Strategic Risk Register
Presented By	Lorraine Grierson
Recommendation	Approval
Appendix Attached	NO
Disclosable Under FOISA	YES

Read Time: 3 minutes

1. Recommendation

1.1 The Finance and General Purposes Committee are asked to approve the Strategic Risks 3 and 7.

Strategic Risk Register

2. Executive Summary

2.1 The purpose of this paper is to provide the Committee with the opportunity to review the College's Strategic Risks associated with FGP Committee.

3. Context

3.1. The Principal and Executive Leadership Team routinely review the Strategic Risk Register to reflect the key risks to the College and the mitigations that will be applied to each risk.

3.2. Currently F&GP Committee has 2 risks assigned to it for review and any amendment made to these is noted below:

- Risk 3 – Failure to Achieve Institutional Sustainability – **no changes**
- Risk 7 – Failure to achieve industrial relations - **no changes**
- Risk 7 will be presented at Audit Committee on 19th September for deep dive discussion.

4. Strategic Implications

4.1 This paper links into the following strategic priorities: Priority 2 – People and culture, Priority 4 – Growth and Financial Sustainability

5. Risk

Risk	**Mitigations**
Risk 3 and Risk 7	Paperwork attached for reference.

6. Implications

Financial	Yes	The College is required to achieve a balanced budget position on an annual basis. Financial loss due to industrial action.
Legal	Yes	Failure could result in insolvency, reputational damage and industrial action.
Learning and Teaching	Yes	Challenges to deliver on the objectives set out in the Regional Outcome Agreement (ROA). Challenges re sustainability of course offerings and impact on industrial action to learning.
Equalities	No	

L Grierson
Secretary to the Board
September 2023

STRATEGIC RISK REGISTER UPDATE F&G COMMITTEE – SEP 23

RISK DEFINITION		ORIGINAL TASK				RESIDUAL RISK					
No	Risk	Likelihood	Impact	Total	Risk Level	Likelihood	Impact	Total	Risk Level	Risk Appetite	Trend
Responsible Person - VP Finance and Commercial Services											
3	Failure to achieve institutional sustainability (F&GP)										
		4	5	20		4	5	20		Averse	=
Responsible Person – VP People and Transformation											
7	Failure to achieve effective Industrial Relations (F&GP)										
		5	4	20		5	3	15		Moderate	=

KEY: ASSESSMENT OF RISKS

Risks which should be monitored by the Risk Management Group:	Scores: 1 – 8	Minor Risk
Risks to be brought to the attention of SMT and the Board of Management:	Scores: 9 - 15	Significant Risk
Risks to be reported to, and monitored by, Board of Management:	Scores: 16 – 20	Major Risk
Risks to be reported to, and monitored by, Board of Management:	Scores: 21 – 25	Fundamental Risk

Risk Score MatrixImpact

5	10	15	20	25
4	8	12	16	20
3	6	9	12	15
2	4	6	8	10
1	2	3	4	5

Likelihood

Strategic Objective: Risk No: 3 Financial Sustainability

Reference to Departmental Risk Registers:	Financial
Owner:	VP Finance, Strategy and Sustainability
Description of the Risk:	Failure to achieve institutional sustainability
What are the possible consequences if the risk was to emerge?	The college will be unable to continue, becomes insolvent, contravening governance requirements by SG, Section 22, Reputational damage to Board and F&GP

Numerical Scoring of Gross Risk (i.e., without controls in place)					
What is the predicted **LIKELIHOOD** of the risk occurring?	(A) 4/5	What is the predicted **IMPACT** of the risk?	(B) 5/5	What is the total risk score? (A x B)	20/25
The **GROSS** risk is therefore: MIN/SIG/MAJ/FUND	**Major Risk**				

3 LINES OF DEFENCE	MITIGATIONS	MONITORING
FRONT LINE (Management Assurance) **Operational Delivery /Systems /Quality Assurance /Supervision**	• Increase commercial income to reduce reliance on SFC funding • Effective cost control • Active tracking of Credits achieved/forecast vs target • Protection of funding through dialogue with SFC	• Regular review of financial strategy and non-core income sensitivity • Finance business partnering to review budgets/spend with Managers • Continuous monitoring of demand v funding allocation of student funds
OVERSIGHT OF MANAGEMENT ACTIVITY **Internal Compliance and quality checks / Legal and Regulatory / Financial controls / Management controls / Project assurance**	• Strategic plan and Operating Plans approved by BoM and Committee • Budgets approved by BoM and Committee • Major project business cases approved by BoM and Committee • Finance Directors Network	• Regular internal reporting to BoM and Committee • Regular interaction with Scottish Funding Council Finance Team • Knowledge exchange through Finance Directors Network / Colleges Scotland • VPs Group and Principals Group
INDEPENDENT ASSURANCE **Internal Audit / external bodies**	• Internal Audit Programme agreed by BoM/Audit Committee • External Auditors appointed through Audit Scotland • Regional Outcome Agreement	• BoM/Committee review and approval of IA reports and action points tracking • Audit Committee/BoM oversight • Regular returns to Scottish Funding Council (FFR/FES)

Numerical Scoring of NET Risk (i.e., with controls in place) (2 cont.)					
What is the predicted **LIKELIHOOD** of the risk occurring?	(A) 4/5	What is the predicted **IMPACT** of the risk?	(B) 5/5	What is the total risk score? (A x B)	20/25

Risk Status	**Meeting 1** **SIG**	**Meeting 2**	**Meeting 3**	**Meeting 4**

MEETING	AMENDMENTS TO RECORD
Q1	No change

Strategic Risk Register

Q2	
Q3	
Q4	

No.	Risk and Risk Appetite	Avoid	Averse	Cautious	Moderate	Open	Hungry
3	Failure to achieve institutional sustainability						

Strategic Risk Register

Strategic Objective:	Risk No: 7

Reference to Departmental Risk Registers:	Organisational
Owner:	Vice Principal People and Transformation.
Description of the Risk:	Failure to achieve effective Industrial Relations
What are the possible consequences if the risk was to emerge?	Financial loss, impact to ability to effectively teach, industrial action, loss of reputation.

Numerical Scoring of Gross Risk (i.e., without controls in place)					
What is the predicted **LIKELIHOOD** of the risk occurring?	(A) 5/5	What is the predicted **IMPACT** of the risk?	(B) 4/5	What is the total risk score? (A x B)	20/25
The **GROSS** risk is therefore: MIN/SIG/MAJ/FUN	**Major Risk**				

3 LINES OF DEFENCE	MITIGATIONS	MONITORING
FRONT LINE (Management Assurance) **Operational Delivery /Systems /Quality Assurance /Supervision**	• Constructive formal and informal communication channels • Regular meetings • Staff awareness and contingency planning	• LJNC • College Employers Scotland advice and updates • Regular union/management dialogue
OVERSIGHT OF MANAGEMENT ACTIVITY **Internal Compliance and quality checks / Legal and Regulatory / Financial controls / Management controls / Project assurance**	• LJNC (Local Joint Negotiation Committee) • Representation at Employers Association • NRPA (National Recognition and Procedures Agreement) • Engagement/practice sharing with local agencies • Attendance at Strategic HR Network	• ELT/SLT/Board • Regular employee engagement monitoring • Regular union/management dialogue •
INDEPENDENT ASSURANCE **Internal Audit / external bodies**	• College Employers Scotland	• SFC/Scottish Government • FGP/BoM oversight

Numerical Scoring of NET Risk (i.e., with controls in place) (2 cont.)					
What is the predicted **LIKELIHOOD** of the risk occurring?	(A) 5/5	What is the predicted **IMPACT** of the risk?	(B) 3/5	What is the total risk score? (A x B)	15/25

Risk Status	Meeting 1	Meeting 2	Meeting 3	Meeting 4
	SIG			

MEETING	AMENDMENTS TO RECORD
Q1	No changes.
Q2	
Q3	
Q4	

Strategic Risk Register

No.	Risk and Risk Appetite	Avoid	Averse	Cautious	Moderate	Open	Hungry
7	Failure to achieve effective Industrial Relations						

DUMFRIES AND GALLOWAY COLLEGE

MEETING	FINANCE AND GENERAL PURPOSE COMMITTEE
Agenda Item:	**5**
Paper No:	**FGP0923-5.1**

Date	13 September 2023
Location	MS Teams On-line
Title of Paper	Terms of Reference / Committee Self Evaluation
Presented By	Lorraine Grierson
Recommendation	Discussion
Appendix Attached	NO
Disclosable Under FOISA	NO

Read Time: 3 minutes

1. Recommendation

- The Finance and General Purposes Committee is asked to note the self-evaluation information
- review and agree the Terms of Reference for Board approval

2. Executive Summary

2.1 The Board of Management is required under the Code of Good Governance for Scotland's Colleges (section D.23) to self-evaluate annually its performance and effectiveness against its overall duties and responsibilities. Compliance with the Code is a condition of grant awarded by SFC. The implementation of robust self-evaluation processes will ensure that governance arrangements are compliant with the Code of Good Governance.

3. Context

3.1 The self evaluation was carried out in May 2023 and the completed evaluation is attached for information. This has previously been sent out to committee members for their comment and approval.

3.2 As part of the evaluation process, the terms of reference also need to be reviewed annually.

3.3 C.7 (D)) of the Code of Good Governance states setting quorum for board and committee members should be set at 50% or higher and ensuring that the majority in any decision making are non-executive members.

3.4 The terms of reference now include the Committee Schedule of Business for each meeting. These have been reviewed by the executive team member/s and are attached for your information and agreement before being submitted to the full board for approval.

4. Strategic Implications

4.1 Board effectiveness impacts on all priorities within Ambition 2025.

5. Risk

5.1 No risks associated with this paper.

6. Implications

Financial	NO	
Legal	NO	
Learning and Teaching	NO	
Equalities	NO	

Lorraine Grierson
Secretary to the Board
23 August 2023

Terms of Reference	Finance & General Purposes Committee
Date Approved by Committee	Nov 2021
Date Approved by Board	Nov 2021
Date of Next Review	Sept 2023
Chair	Richard Nash

Membership

1.1. Minimum of 3 non-executive board members (one of whom shall be appointed as Committee Chair).

1.2. Chair of the Finance & General Purposes Committee (F&GP) is precluded from serving on the Audit Committee.

1.3. The Principal

1.4. 1-2 Staff Members

1.5. It is desirable that at least one member should have a background in finance, accounting/audit and HR.

1.6. In attendance:

1.6.1.1. Executive Director of Finance

1.6.1.2. Depute Principal of Learning Skills & Student Experience

1.6.1.3. Vice Principal of People & Transformation

1.6.1.4. Secretary to the Board

2. Quorum

2.1 No less than one half of the members entitled to vote. (quorum 50% or higher of membership, with the majority for decision-making to be non-executives).

3. Reporting

3.1. The F&GP shall make its recommendations to the Board of Management as appropriate.

3.2. The F&GP shall observe the Standing Orders in all its business.

3.3. Minutes of the meetings should be circulated to the Board for information.

4. Responsibilities

4.1. Financial Management

4.1.1. Consider the annual budget and recommend approval to the full Board.

4.1.2. Monitor actual performance against budget and provide an update to the Board on financial sustainability.

4.1.3. Consider capital expenditure, investments and borrowing in accordance with Scottish Funding Council (SFC) guidance and recommend approval to the full board.

4.1.4. Consider the Financial Forecast Return (FFR) to SFC and recommend approval to the full Board.

4.1.5. Consider the annual statutory accounts and recommend approval to the Audit Committee.

4.1.6. Oversee systems of financial control and delegated authority.

4.1.7. Carry out the Board of Management's constitutional delegation in financial matters.

4.1.8. Ensure compliance with the Financial Memorandum and Financial Regulations.

4.1.9. Consider and make recommendations for the Finance and Performance Strategy and monitor performance against KPIs at least once a year before presentation to the Board.

4.1.10 Monitor the strategic risks relevant to the Committee and suggest recommendations as required.

4.2. **Estates and Infrastructure**

4.2.1. Consider and make recommendations for the Systems and Infrastructure Strategy and monitor performance against KPIs at least once a year before presentation to the Board.

4.2.2. Review the estates strategy, to ensure infrastructure is fit for purpose and sustainable.

4.2.3. Make recommendations to the Board on matters relating to the development and management of its property and facilities

4.2.4. Consider and make recommendations for the annual report on estates, sustainability and health and safety aspects of the College's operations where these relate to estates and facilities.

4.3. **Commercial and Marketing**

4.3.1. Consider and make recommendations for Business Development and Marketing and monitor performance against KPIs quarterly before presentation to the Board.

4.3.2. Consider and make recommendations for the annual report on Business Development and Marketing and monitor performance against KPIs on strategy out-turn.

4.4. **Human Resources, Organisational Development and Transformation** *(The People and Transformation element will be heard at the HR Sub Committee and reported back to FGP)*

4.4.1. Ensure the College is operating within all legal requirements relating to employment law and other legislation affecting employment.

4.4.2. Agree and approve the People and Culture Strategy monitoring performance against KPIs and recommend any action to the Board.

4.4.3. Ensure appropriate arrangements are in place for effective dialogue with trade unions.

4.4.4. Ensure appropriate policies are in place for staff related matters e.g. appointments, promotion, staff development and appraisal and succession planning.

4.4.5. Review Equality and Diversity updates and the Annual Report, monitoring the College's progress in the implementation.

4.4.6. Monitor and review cyber resilience and information security capabilities to ensure IT infrastructure and information is protected and strengthened to ensure compliance with legislative requirements, and to ensure digital provision is fit for purpose and sustainable.

4.4.7. Monitor and review Data Protection and privacy processes, and staff training to ensure compliance with legislative requirements.

4.5. **Other**

4.6. Undertake a self-evaluation exercise and review of the terms of reference annually to ensure that the Committee complies with best practice in relation to governance. Any amendments to the terms of reference shall be submitted to the Board of Management for consideration and final approval

4.7. **Meetings**

The F&GP will normally meet at least four times per year.

4.8. **FGP Schedule of Business**

Standing Items:

- Maintain minutes and report to board
- Review F&GP Action Log
- Review Risk Register and mitigating actions
- Financial Update (Management Accounts/Contribution Report)
- HR update – progress against KPIs
- Information Governance update – progress against KPIs
- Estates And Sustainability update – progress against KPIs
- Equality & Diversity update
- Business Development and Marketing Update

Meeting 1 (Aug-Oct) Q1	Meeting 2 (Nov-Jan) Q2	Meeting 3 (Feb-April) Q3	Meeting 4 (May-July) Q4
➢ Bad debts >£1000/Scheme of Delegation (when required ➢ Review Year End Return ➢ Review internal strategies ➢ Business Development and Marketing Annual Report	➢ Approve Statutory Accounts to recommend to the Audit Committee ➢ Estates and Sustainability Annual Report to include Carbon Management Data	➢ Equalities & Diversity Annual Report (Statutory Report every 2yrs – due 2025) ➢ Approve Mid-year FFR (current year progress) ➢ Review Draft Budget for next AY	➢ Approve budget submission ➢ Committee Self-evaluation and review of Terms of Reference/ Business Schedule ➢ Approve full FFR (5 year budget forecast) ➢ Review ICT Security and ICT Acceptable Use Policies every 3 yrs if required.

FGP COMMITTEE EVALUATION

(to be completed by Committee Members collectively)

Date: 8/6/23

Section	Yes	No	N/A	Comments/Action
Composition, Establishment and Duties of the Committee				
Does the Committee meet regularly in accordance with the Board Standing Orders?	Y			
Does the Committee consistently have a quorum?	Y			
Do all Committee members attend meetings regularly?	Y			
Does the Committee have enough members?	Y			
Does at least one of the Committee members have a background relevant to the remit of the Committee?	Y			
Have new Committee members received all necessary training?	Y			
Does the Committee report regularly to the Board?	Y			

Section	Yes	No	N/A	Comments/Action
Terms of reference				
Does the Committee have written terms of reference?	Y			
Do the terms of reference include all aspects of the Committee's role?	Y			
Does the membership of the Committee need to be changed?		N		
Are the terms of reference adopted by the full Board and reviewed annually?	Y			

Section	Yes	No	NA	Comments/Action
Compliance with the Law and Regulations				
Does the Committee have a mechanism to keep it aware of topical legal and regulatory issues?				

Section	Yes	No	NA	Comments/Action
Internal Control				
Does the Committee monitor to ensure that risk is controlled?	Y			
Does the Committee regularly review relevant strategic plans?	Y			
Does the Committee consider the level of detail and information it receives appropriate?	Y			
Are appropriate internal performance measures monitored by the Committee?				
Is the Committee addressing all matters delegated to it by the	Y			

Board and under its terms of reference?				

Section	Yes	No	NA	Comments/Action
Administrative arrangements				
Does the Committee have an independent secretary?	Y			
Are Committee papers distributed in sufficient time for members to give them due consideration?	Y			
Are Committee meetings scheduled prior to important decisions on specific matters being made?	Y			
Is the timing of Committee meetings discussed with all involved?				

DUMFRIES & GALLOWAY COLLEGE

MEETING	Finance & General Purposes Committee
Agenda Item:	**7**
Paper No:	**FGP0923-7.3**

Date	13/09/2023
Location	MS Teams On-line
Title of Paper	ICT Security Policy and ICT Acceptable Use Policy
Presented By	Calum Rodgers
Recommendation	**Discussion**
Appendix Attached	YES
Disclosable Under FOISA	YES

Read Time: 5 minutes

1. Recommendation

1.1 The Finance and General Purposes Committee are asked to approve the changes to the ICT Security Policy and the ICT Acceptable Use Policy.

2. Executive Summary

2.1 The ICT Security Policy and the ICT Acceptable Use Policy have been updated under the review cycle for College Policies and Procedures.

2.2 The ICT Security Policy has had paragraph 6.2.13 added to include guidance on USB drives.

2.3 The ICT Acceptable Use Policy has been fully revised to update it. A guidance note for a student friendly version has been created.

3. Context

3.1 The ICT Security Policy has been revised to ensure it reflects changes to DGC management, security and protection of all ICT systems and data.

3.2 Following an audit recommendation from 2021 a paragraph on the safe use of USB drives has been added.

3.3 The ICT Acceptable Use Policy has been revised to ensure that it reflects current legislation and guidance. This aligns it to the Scottish Government Public Sector Action Plan for Cyber Resilience. A guidance note for a student friendly version of the ICT AUP has been created. This will be published on the student portal and will sign post to the main ICT AUP.

4. Strategic Implications

4.1 This paper is linked to Strategic Priority 5 - Systems and Infrastructure.

5. Risk

Risk	Mitigations
11 – Failure to achieve and maintain systems and operable and secure ICT	➢ College procedure for ICT security detailed including backup and business continuity. ➢ Clear guidance on expected behaviour of both staff and students published.

6. Implications

Financial	No	No direct financial implications
Legal	Yes	Compliance with UK GDPR and the Data Protection Act 2018 (DPA 2018) and the Privacy and Electronic Communications Regulation 2003 (PECR 2003).

Learning and Teaching	No	No direct Learning and Teaching implications.
Equalities	No	No direct Equalities implications.

Calum Rodgers
ICT Manager
September 2023

Dumfries and Galloway College
One step ahead

ICT ACCEPTABLE USE POLICY

Responsibility: Vice Principal, People and Transformation

Issue Date:

Equality Impact Assessment: 28.08.23

Version: 1

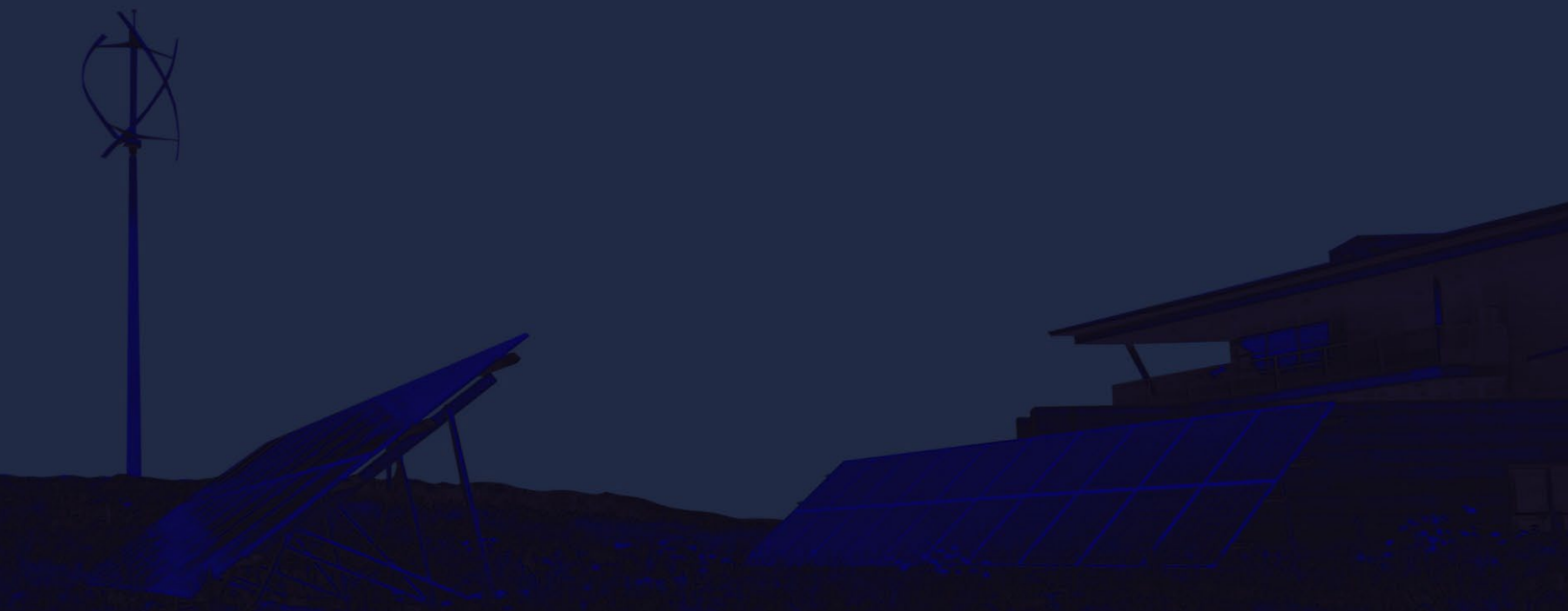

Table of Contents

ICT Acceptable Use Policy

1. Purpose

The policy is intended to protect users and their data, and the College from illegal or damaging actions by individuals, either knowingly or unknowingly. Ignorance of this policy (or those that it directs you to), and the responsibilities it places on you, is not an excuse in any situation where it is assessed that you have breached the policy and its requirements.

Inappropriate use by individuals will be managed in accordance with College policies and procedures, including the Disciplinary Policy and the Code of Student Behaviour.

It will also be reported to law enforcement agencies if appropriate.

The aim of the Dumfries and Galloway College Acceptable Use Policy (AUP) is to reflect the established culture of openness, trust, and integrity.

The purpose of this policy is to outline the acceptable (and prohibited) use of college computer equipment and network access. Inappropriate use exposes the College to a range of risks including virus attacks, compromise of network systems and services, and legal issues. This policy also prohibits accessing College ICT facilities to cause harm or offense to others.

There needs to be commitment to protect Dumfries and Galloway College employees, students, Academic partners, and the wider Joint Academic Network (JANET) organisation from illegal or damaging action by individuals, either knowingly or unknowingly.

All internet access originating from the College network is subject to the JANET Acceptable Use Policy: https://community.jisc.ac.uk/library/acceptable-use-policy.

2. Scope

This policy applies to all users including staff, students, Board of Management, contractors, consultants, temporaries, and other workers at Dumfries and Galloway College, including all personnel affiliated with third parties.

This policy applies to all equipment that is owned or leased by Dumfries and Galloway College and to all equipment connected to the College's network.

Students and staff who connect their own devices to the College's network and the services available require compliance to this policy.

Use of Dumfries and Galloway College ICT equipment and the Dumfries and Galloway College network are limited to staff, students and authorised third parties only.

3. References

This policy is aligned with other policies and procedures within the College, namely:

- Data Protection Policy
- ICT Security Policy
- Learner Behaviour Policy
- Equality and Diversity Policy
- Data Breach Procedure
- Student Disciplinary Procedure

4. *Definitions*

- AUP – Acceptable Use Policy
- ICT – Information & Communication Technology
- Spoofing – pertaining to be from another user
- Proxy/Proxies – system that facilitates data exchange between networks
- VPN – Virtual Private Network
- VLE – Virtual Learning Environment (LearnNet)
- MFA – Multi Factor Authentication
- PII - Personally Identifiable Information

5. *Responsibility*

The responsibility for the supervision of the Acceptable Use Policy is delegated to the ICT Manager. Any suspected breach of this policy should be reported to a member of Digital Services staff. The Vice Principal, People and Transformation will then take the appropriate action.

Actions will include, where relevant, immediate removal from online information systems of material that is believed to infringe the law. The College reserves the right to audit and/or suspend without notice any account pending any enquiry. Where necessary, this will include the right to intercept communications.

This policy is not exhaustive and inevitably new social and technical developments will lead to further uses, which are not fully covered here at present. In the first instance students should address questions concerning what is acceptable to their personal tutor. Staff should approach their line manager. Where there is any doubt, the matter should be raised the Digital Services Helpdesk, who will ensure that all questions are dealt with at the appropriate level within the College.

6. Policy

6.1 Disciplinary Procedures

Staff and students who contravene this policy may find themselves subject to the College's disciplinary procedures.

Individuals may also be subject to criminal proceedings. The College reserves its right to take legal action against individuals who cause it to be involved in legal proceedings as a result of their violation of licensing agreements and/or other contraventions of this policy.

6.2 Authorisation and Conditions of Use

6.2.1 Authorisation

Users are provided access to the College ICT Systems when they meet the following categories:

- Members of staff.
- Students.
- Partners of the College (i.e., learning network staff, individuals on work experience, contractors, auditors etc.)

Access will not be restricted on the grounds of disability, impairment or any other protected characteristic.

By logging on to a College system, whether on premise or remotely, users are confirming acceptance of this policy by either clicking accept or ticking an acceptance button prior to logon.

When staff employment or a course of study finishes, access to ICT resources will be revoked automatically and the user accounts will be closed as per internal procedures.

6.2.2 Conditions of Use

ICT resources and Information Systems are provided primarily to support College business such as teaching, training, study, and administrative support of these activities. However, reasonable personal use is also permitted provided there is compliance with this policy. Individuals should exercise due care and attention whilst using College ICT resources to ensure that the corporate reputation remains a priority and no inflammatory posts could be attributed to the College on either internal or external information systems or social media.

Users must not masquerade as someone else and should always keep their logon identity and password private (exceptions will be made for users who have additional support needs). Users should choose a hard to guess password, of which guidance can be found within the College password change procedure which is available from the intranet.

Each user has a personal duty to follow the AUP as diligently as possible, in most cases the College will prefer to inform users of a contravention to the AUP informally while advising corrective action. However, repeated or a serious breach to the AUP will trigger disciplinary procedures.

The following acts can be construed as a misuse and a breach of the AUP:

- Installing software that is not explicitly permitted by the ICT Department.
- The printing, displaying, storing, internet browsing or transmitting of unacceptable or offensive material. This will include material which is:
  - Racially, religiously, sexually, or politically offensive.
  - Obscene, indecent, or pornographic.
  - Likely to promote terrorism or violence.
- The creation or transmission of material which is intentionally designed or likely to cause annoyance, inconvenience, intimidation, or anxiety. This includes cyber- bullying or harassment in any form. Users should ensure that appropriate language and tone should be used in communications at all times in line with College policies and procedures.
- Intentionally affecting security systems or the disruption of network communications, including:
  - Intentionally clicking on known malicious links or running malicious software.

- Implementing a Denial-of-Service attack.
- Excessive or inappropriate use of College network bandwidth.
- Port scanning or information gathering (reconnaissance activity) of network systems exercises.
- Network monitoring/sniffing.
- Providing information about users outwith the College.
- An attack that intentionally disrupts, prevents and/or removes access to computing services within the College or any external organisation.
- Circumventing user authentication or security of any host, network, or account.

- Unauthorised copying, including downloading from the internet, of copyrighted material including, but not limited to, digitisation of photographs from magazines, books, music, applications, or other copyrighted sources.
- Utilising 'proxies' or VPN services to circumvent the College security systems.
- Using computer resources to commit fraud, deception, or another criminal act.
- Vandalism of deliberate physical damage to College equipment.
- Accessing another user's account.
- Impersonating another user whether real (via the user account) or artificial (spoofing). For example, sending messages that appear to originate from another person.
- Sending chain or bulk ('spam') messages.
- Use of College systems for commercial gain, running a business, non-College related advertising, crypto mining, or political lobbying.
- Using unauthorised or unlicensed applications including games, screensavers, drivers, browsers, and plug-ins.
- Adding hardware devices to the College network without explicit authorisation from the Digital Services Department.
- Introducing viruses or malware (e.g., viruses, worms, Trojan horses) designed to impact systems performance, integrity, security, availability to harvest data.
- Breaching or attempting to breach security controls including:
  - Interfering with or disabling anti-virus software.
  - Attempting to change 'safe search' settings.
  - Disabling Windows/Mac update services.
  - Encrypting key College data/systems without authorisation.

- Changing system policies which reduces security (firewalls, modifying logs, disabling encryption on managed devices, etc).

- Any action, or lack of action, which may interfere with the security of College systems or a data breach of Personally Identifiable Information (PII) or sensitive data as per the Data Protection Act 2018 and the General Data Protection Regulations (GDPR).
- Exporting, processing, or transfer of other users' PII or sensitive data outside of secure College systems.
- Contravening the JANET AUP (as referenced on page 3).

It is important that any personal data breaches, or indeed suspected breaches, across the College are reported as soon as possible to the Vice Principal People and Transformation and the Data Protection Officer College as per the Data Breach procedure.

Under the terms of the Data Protection legislation, data controllers have no longer than 72 hours to report a breach to the Information Commissioner's Office after having become aware of it. The College will abide by this statutory requirement.

6.3 Accessing Services or Data Remotely (including on-campus mobile devices)

The College provides several services (email, files, VLE, intranet, etc.) which can be accessed remotely or via guest Wi-Fi services such as Eduroam.

It should be noted that the Internet Protocol (IP), MAC address and browser version data may be recorded when using these systems. This means that location and device browser information can be harvested.

The following requirements shall also apply to user remotely accessing services and data:

Applies to all users:

- Users shall only access any remote services using a device that continues to receive security updates from the vendor and ensure that security patches are applied within 14 days of release.
- Devices should have adequate and up-to-date anti-virus/malware software installed.

Applies to Staff and Partners only (not Students):

- In line with the College Data Breach procedure, it is important that individuals inform the Digital Services Helpdesk immediately if a mobile device (whether College owned or personal) that has been used to access College data is lost or stolen. The Digital Services Helpdesk will take steps to attempt to remotely wipe College data and apply measures to minimise the potential for data loss. The Digital Services Helpdesk will notify the Vice Principal People and Transformation, the Data Protection Officer, or a member of the Senior Leadership Team if a personal device containing data has been lost or stolen.
- It is strongly recommended that mobile devices are encrypted and are protected with a pin of at least 8 digits.
- Accessing College systems/data is not permitted on personal devices outside of the European Economic Area.
- Any application used on a mobile device must be downloaded from either the Apple App Store or Google Play Store (no 'jailbroken' devices should be used).
- Any devices accessing core or critical data/applications (HR data, Student Records, payroll) must be connected using a College encrypted laptop and Virtual Private network (VPN).
- If using a College owned mobile phone/tablet, the device must be enrolled in the Mobile Device Management system.
- Individuals should use College assigned storage to store, transfer, process, and access required data.
- PII data should never be sent outside of the College via email. If you need to send PII data external to the College then you must ensure:
  - There is a data sharing agreement in place.
  - The data file is suitably encrypted.
  - The data is shared and transferred using approved processes then unshared once the transfer has been completed.

6.4 Key Principles

6.4.1 Filtering

The College utilises automated recording, filtering, and monitoring software (Spam filter, URL filters, application filters, file auditing, administrative auditing software, etc.) to protect College systems, user data and other sensitive information. These cannot be guaranteed failsafe and users have a responsibility to be vigilant when using College systems and processing data.

Opening emails and browsing websites should always be carried out with diligence and care. The College will filter and attempt to scan and block content or Internet activity which is deemed as being unsuitable or malicious, containing viruses or exploits. This includes pornographic, gambling and sites that provide a security threat.

The College appreciates the cooperation from users and promotes a reporting culture with regards to Cyber incidents. Users are asked to inform Digital Services if they receive a suspicious email or notice irregular activity on their devices. Contact should be made to digitalservices@dumgal.ac.uk

6.4.2 Email

College email addresses and associated College email systems must be used for all official College business, to support audit purposes and institutional record keeping. All staff and students at the College must regularly read their College email and delete unwanted or unnecessary emails at regular intervals.

It is not permitted to use personal email accounts for work purposes at any time. Personal email accounts do not have the same level of security as College accounts and as such provide a serious risk to the Colleges networks.

6.4.3 Cyber Security

Cyber-attacks are an increasing threat to organisations. The attacks are mostly initiated through the theft of user credentials. Essentially attackers view people as being vulnerable and open to exploitation.

The College has taken steps to increase the understanding of staff around cyber security, which will ensure the College is better protected and that staff can better protect their personal digital identity outside of the College.

The College has introduced Multi Factor Authentication (MFA) for remote access on all College staff accounts. Use of MFA on personal accounts is strongly recommended (e.g., Gmail, Facebook, Twitter, and other social accounts).

Information relating to MFA will be routinely provided by the Digital Services Team.

6.4.4 Social Media

The College recognises the role that social networking and other communication technologies holds within modern student life and learning and teaching practice.

The College will use social media in curriculum delivery, particularly in terms of communications with students, gaining feedback, and group discussion; and, for corporate communication, marketing, and promotion and for contact with the business community.

Social Media sites used for corporate communication, marketing and promotion will be managed by the Marketing Team. All staff members using social networking sites as tools through which to communicate with students must only do so on a professional basis. Guidance on use of social can be found in the social media guidelines in the quality manual on AdminNet and LearnNet.

6.4.5 Copyright Compliance

Employees and students must not download, copy or otherwise re-produce material for which they have not obtained permission from the relevant copyright owner.

If such material is required for any purpose e.g., teaching or research, then copyright permission must be obtained and documented before such material is used.

Employees and students are reminded that the College treats plagiarism very seriously and will investigate any allegation i.e., the intentional use of other people's material without attribution.

6.4.6 Monitoring

While the College Digital Services department aims to provide a high level of privacy all, users should be aware that the data they create on the College systems remains the property of the College.

Dumfries and Galloway College reserve the right to audit networks and systems on a periodic basis to ensure compliance with this policy. Systems are monitored to ensure that the confidentiality, integrity and availability of systems and data is maintained.

Users should be aware that data held within the College is not routinely inspected and user data will normally be treated as confidential. An examination of user data will only be carried out in response to an alleged violation to the AUP or for governance/legal reasons such as GDPR compliance or Police Investigation.

The College recognises that it has a duty of care in such investigatory work.
It should also be noted that when accessing College systems remotely your IP address is recorded and can be used responsibly by College security systems to prevent malicious activity; this can be with automated alerting systems or pro-actively by the Digital Services department.

The data the College collects, is subject to its processes and retention periods, these can be found in the College Data Protection Policy.
https://board.dumgal.ac.uk/dg_file/data-protection-policy/

Line managers of staff who leave the College will receive access to emails and files to ensure no important data is purged as a consequence of an individual leaving its employment.

To ensure business operations it may also be necessary to grant line managers access to staff files/emails if they are on prolonged sick or annual leave. Formal approval will be sought from SLT before access is granted.

6.5 Relevant Legislation

- Copyright, Designs and Patents Act 1988
- Malicious Communications Act 2003
- Computer Misuse Act 1990
- Trademarks Act 1994
- Data Protection Act 2018
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Freedom of Information (Scotland) Act 2002

6.6 External Guidance

National Cyber Security Centre, Cyber Essentials Plus Accreditation
https://www.ncsc.gov.uk/cyberessentials/overview

Scottish Government Public Sector Action Plan for Cyber Resilience
https://www.gov.scot/publications/cyber-resilience-strategy-scotland-public-sector-action-plan-2017-18/

7. Distribution

All Staff
Repository

8. Revision Log

Revision Log		
Date	Section	Description
May 2023	Throughout the Policy	Complete rework of policy to reflect current legislation and guidance
May 2023	Throughout the Policy	Numbering changed to comply with Document Control Procedure
May 2023	Distribution	Quality Manual changed to Repository
May 2023	Responsibility	Job Title changed from Vice Principal Business Development and Corporate Services to Vice Principal, People and Transformation
June 2023	Appendix	Student Friendly AUP Guidance Note added as Appendix 2

THIS FORM TO BE UPDATED WHENEVER THERE IS A CHANGE IN ANY SYSTEM DOCUMENT				
Document Name	Document Owner	Revision Number	Date of Issue	Date of Withdraw
ICT Acceptable Use Policy	Vice Principal, People and Transformation	1		

Appendix 1: Equality Impact Assessment

Document:	ICT Acceptable Use Policy
Executive Summary:	Impacts are positive across all of the protected characteristics for this policy as it will discourage online bullying and harassment or other inappropriate use which might create an intimidating culture within the college. This applies less clearly to the additional considerations, although impacts should still be mildly positive as people from the groups listed can find themselves marginalised and excluded, which the policy should help to discourage. The Human Right to privacy and family life is protected through restricted use of monitoring and data protection measures built into the policy.

Duties:
1: Eliminate discrimination, harassment, and victimisation
2: Promote equality of opportunity
3: Promote good relations
* Human Rights to privacy and family life, freedom of thought and conscience, education, employment

PSED Impacts

	Commentary
Age	The policy discourages online bullying and harassment, which can disproportionately affect people in minority groups across the protected characteristics. Prevention and reduced risk of this kind of negative behaviour will promote good relations.
Disability	
Gender	
Gender Based Violence	
Gender identity/ reassignment	
Marriage/civil partnership	

Pregnancy/maternity	
Religion or Belief	
Race	
Sexual Orientation	

Additional Considerations

Care experienced	The policy discourages online bullying and harassment, which can be a problem for people across the range of additional considerations as they can be marginalised and isolated. The policy should encourage respect and instil confidence in people from these groups.
Carers	
Mental Health	
Socio-economic status	
Veterans	
Human Rights*	The Human Right to privacy and family life is protected through restricted use of monitoring and data protection measures built into the policy. Rights to Education and Employment are positively impacted given that continued engagement in a course which might have been impacted by negative online behaviours of others is minimised.

Lead Officer:	Vice Principal, People and Transformation		
Facilitator:	ICT Manager		
Date initiated:	06.06.23		
Consultation:			
Research:			
Signature	*Calum Rodgers*	Date	28.08.23

Appendix 2. Student Friendly AUP Guidance Note

This it to be displayed on the Student portal, linked in LearnNet and referenced in the student induction.

The following acts will be considered misuse of College services and a breach of the ICT (Information and Communication Technology) Acceptable Use Policy:

- Installing any software without the permission of the ICT Department.
- Accessing in any form, unacceptable or offensive material including anything that can be considered racially, religiously, sexually, or politically offensive.
- Cyber- bullying or harassment in any form.
- Intentional damage to College ICT equipment.
- Intentionally affecting ICT security systems or the disruption of network.
- Using another user's login information to access College resources.
- Use of College systems for non-college related purposes.

All internet traffic is logged and monitored.

The full ICT Acceptable Use Policy can be found here: [LINK TO MAIN POLICY]

Dumfries and Galloway College
One step ahead

ICT SECURITY POLICY

Responsibility: Vice Principal, People and Transformation

Issue Date:

Equality Impact Assessment: 28.08.23

Version: 2

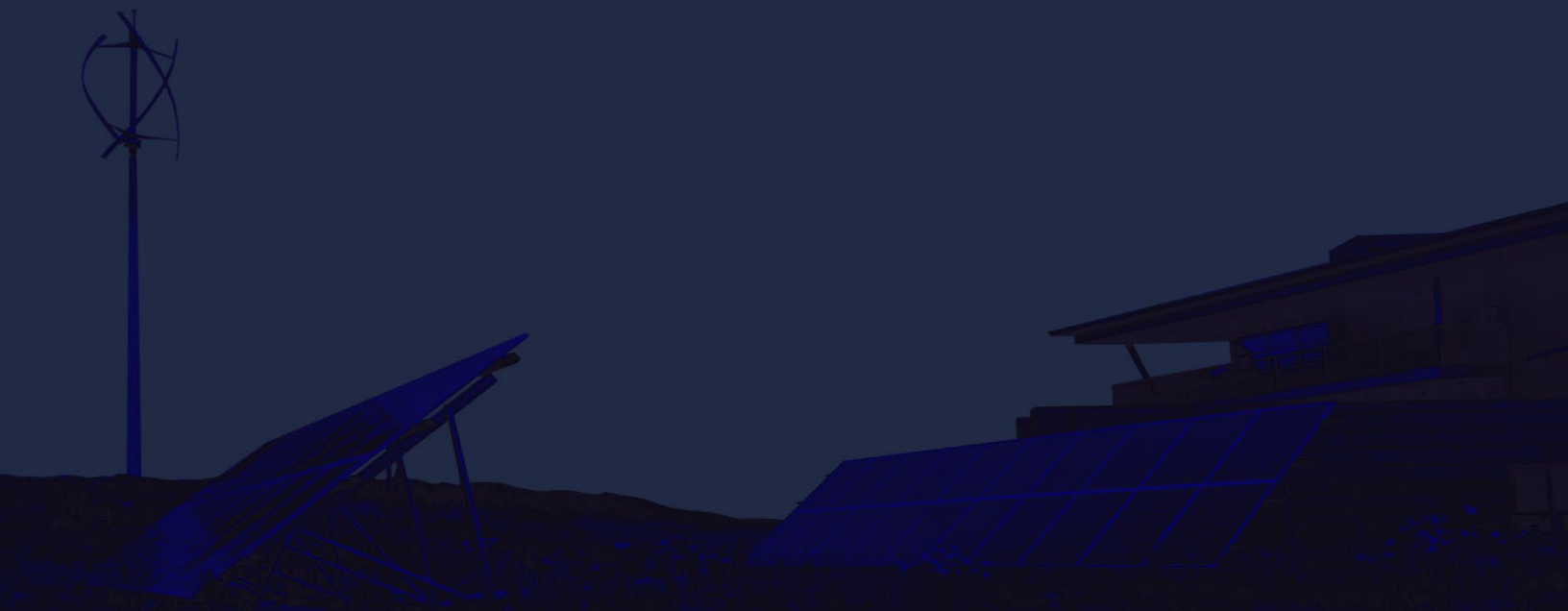

Table of Contents

ICT Security Policy

1. Purpose

The purpose and benefits of this policy are to raise awareness and clearly inform how Dumfries and Galloway College manages, secures, and protects its Information and Communication Technology systems and data.

2. Scope

This procedure is to be implemented at all College sites and applies to all College staff, student and third parties who manage data and services for or on behalf of the College

3. References

The policy is aligned with other policies within the College, namely:

- Data Protection Policy
- Code of Conduct Policy
- Equality and Diversity Policy
- Student Behaviour Policy
- Risk Management Policy

4. Definitions

ICT	Information Communications Technology.
Processes	A series of actions taken to accomplish a goal.
Procedures	An agreed way of completing a task.
Standards	A stated level of acceptance.
Guidance	Help and advice on how to achieve a goal.

5. *Responsibility*

Role	Responsibilities
Senior Leadership Team	Initiate, Define and Authorise Policy
ICT Manager	Creating Procedures, Standards and Controls
ICT Staff	Implement Procedures, Standards and Controls
ICT Users	Be familiar with and adhere to the ICT Security Policy at all times.

6. *Procedure*

6.1 Core

All persons involved with College ICT systems and information must read and comply with these policies.

6.1.1 Information Security

Documents the governing body's direction on and commitment to information security and communicate it to all relevant individuals.

- The Information Security Policy supports the College and IT strategic visions by defining the high-level approach taken to reducing associated risks to its reputation, finances, and operations.
- Information managed by the College shall be appropriately secured to protect confidentiality, integrity, and availability.
- Information will be managed so that the College can ensure appropriate legal, regulatory, and contractual obligations are complied with.
- The College will develop and communicate information security policies, processes, and procedures that all staff, students and third parties are required to comply with.

- The College acknowledges that information security is the responsibility of every member of staff, student and third parties. The College is committed to a programme of awareness, training, and education to address this.

6.1.2 Data Risk Classification

To determine the level of protection that should be applied to types of information, thereby preventing unauthorised disclosure an information classification scheme should be established that applies throughout the organisation, based on the confidentiality of each piece of information.

- All College staff, students and third parties who store, process, transmit and share information on behalf of the College have a personal responsibility for ensuring that appropriate security controls are applied.

- Appropriate security controls vary according to the classification of the information.

- All College information must have a classification assigned by the owner.

6.1.2 Data Handling

To protect information contained in documents in accordance with legal requirements, ensure critical information remains available when required, preserve the integrity of critical information, and protect sensitive information from unauthorised disclosure.

- The College will ensure appropriate security controls for the handling of data are in place by providing secure services for the creation, storage, processing, transferring, sharing, and deleting of information.
- A service catalogue will be maintained and available for users to search.
- Services will clearly state what classification of information can be used with them.
- All users of a service will comply with any processes and procedures as a requirement of using the services.

6.2 User

If you use College managed network connected devices and services, then you must read and comply with these policies.

6.2.1 Acceptable Use Policy

To ensure users are legally and contractually bound to protect the organisation's information, business applications and systems, and the organisation's security obligations are met.

6.2.2 Identification

Unique IT Accounts are associated with each User. These accounts are used to grant specific access to services and information associated with the Users role. Those who have received an IT Account from the College must not:

- Share their IT account or use another Users IT account.
- Disclosed their password to anyone, even College staff.
- Use your IT account username or password to register for non-College services.

6.2.3 Information & Software

The College provides managed software to create, access, process, transfer, share and delete information. Users must ensure that they:

- Comply with the Data Protection Policy.
- Do not cause a breach in confidentiality.
- Do not cause a breach in copyright law.
- Do not cause a breach in licences or contracts.

6.2.4 Email

College email addresses and associated College email systems must be used for all official College business, in order to support audit purposes and institutional record keeping. All staff and students of the College must regularly read their College email and archive or delete unwanted or unnecessary emails at regular intervals.

It is not permitted to use personal email accounts for work purposes at any time. Personal email accounts do not have the same level of security as College accounts and as such provide a serious risk to the Colleges networks.

6.2.5 College owned devices / equipment / services

The College provides computing and communication devices, specialist equipment and information services to support the educational, research, administrative and business functions of the College.

Personal use of College devices is permitted under these conditions:

- Activities are lawful.
- At the user's own risk.
- Withdrawn if deemed to be excessive.
- Must not interfere with contractual, professional, course or research obligations.
- Must not hinder the use of others.

Prohibited use:

- Personal commercial activity.
- Access or disseminating material of a pornographic, criminal, or offensive nature including material promoting terrorism except when prior written authorisation has been granted by the appropriate body.

6.2.6 Consumer devices / equipment / services

Users may use personal consumer devices to access College resources where authorised by the appropriate body. Only information classified as Low risk can be used with consumer devices, equipment, and services.

By doing so the User agrees to the following:

- The College retains the rights to inspect, conduct a remote audit, and remotely wipe the device.
- All College information stored on a consumer device remains the property of the College.
- The waiver of College liability.
- Not to share the device with other individuals.

- Manage the device in accordance with the ICT Security Policy, Management, End User Computing section.

6.2.7 Responsibilities

All Users have responsibilities to protect the confidentiality, integrity and availability of College information. These include:

- Report information incidents promptly: breaches of confidentiality, failures of integrity and loss of availability.
- Provide physical security of mobile devices.
- Report loss or theft of devices.
- Change passwords on notification of compromise.

6.2.8 Monitoring and Logging

The College may monitor communications, files and emails as detailed in the Monitoring and Logging sections within the ICT Security Policy.

6.2.9 Disciplinary

Any breach of this policy can result in disciplinary action.

6.2.10 User Password

To prevent unauthorised users from gaining access to password-protected critical or sensitive information, business applications, systems, networks or computing devices.

- College usernames and passwords are unique and used to grant access to information and resources specific to individual needs.
- They are used to identify and log user activity on College systems and services.
- Passwords must be kept confidential, they should never be shared or disclosed to anyone, the College will never ask for your password.
- A password used to access College resources must not be used to access any external third-party resources.

- Users must report and change passwords if it has been, or it is suspected that it has been compromised.

6.2.11 Remote Working

The College appreciates that there may be circumstances where remote working is required. In normal circumstances this will be facilitated using a college issued devices which has been fully configured for security purposes. We do though appreciate that there may be times where the use of home devices may be required though we expect these would be exceptional circumstances.

To ensure that critical and sensitive information handled by staff working in remote environments is protected against the full range of security threats.
To protect College information from security threats staff working from home or other remote locations should:

- Be authorised to do so.
- Have received relevant security training.
- Do so from an approved secure device.
- Do so by an approved and authorised process.

All devices should be protected against loss or theft by using an appropriate access control mechanism, encryption at rest and in transit, and for mobile devices (e.g. laptop) a tamper proof label with device identification details.

6.2.12 Clean Desk

To ensure information stored in or processed by office equipment is not disclosed to unauthorised individuals.

- All sensitive/confidential information in hardcopy or electronic form is secured in workspace at the end of the day or when unoccupied for an extended period.

- Computer screens must be locked when workspace is unoccupied.

- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.

- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

- Laptops must be either locked with a locking cable or locked away in a drawer when not in use.

6.2.13 USB Guidance

The use of USB drives is permitted on college devices however the guidance below is to be adhered to. It is recommended that users do not store their only copy of files on a USB drive.

Sensitive Data – The storing of sensitive data on a USB drive is only permitted when using an encrypted drive. The password set must not be shared with anyone unless in the event of an investigatory requirement. Once there is no longer a requirement for it to be stored it must be deleted. If the USB drive is lost or misplaced it must be reported to the Data Protection Officer immediately.

Non-Sensitive Data – The storing on non-sensitive data is allowed on any type of USB drive however considerations should still be made as what you store on it and the impact if you were to lose it.

Your Own Data – The storing of an individual's own personal data is allowed on any type of USB drive. Please note that when connecting a USB drive it will scan for any possible threats and if found remove them from the drive. This could include any files you require on a personal level.

6.3 Management

If you manage a device or service which is connected to the network, then you must read and comply with these policies.

6.3.1 End Point Security

6.3.1.1 Physical Security

To restrict physical access to authorised individuals, ensure that critical equipment is available when required and to prevent important services from being disrupted by loss of, or damage to equipment or facilities.

- Physical access to critical facilities, such as data centres, network and telecommunication equipment should be restricted to authorised personnel.
- Authorisation should be issued in accordance with a documented process, be reviewed regularly and revoked promptly when no longer required.
- All visitors to critical facilities must be supervised at all times.
- Environmental and power protections should be in place when required.

6.3.1.2 Network Connection

To prevent unauthorised users or devices from gaining access to information systems and networks.
To ensure that the configuration of network devices is accurate and does not compromise the security of the network.

- All network connected devices must be authorised and managed by a competent authority.
- Must meet the appropriate security standards to protect against the compromise of confidentiality, integrity, and availability of the information that they process.
- Network attached devices should be appropriately resourced to manage their current and predicted processing requirements and segregated

appropriately where necessary.

- Segregated appropriately where necessary.

6.3.1.3 End User Computing

To ensure end user computing devices operate as intended and do not compromise the security of computer installations or other environments.

All end user computing devices that connect to College services and access College information with a classification of "Medium" or "High" must be actively managed by a competent authority and at a minimum comply with the following policies:

- Firewall
- Malware Protection
- Patch Management
- Service Password Management
- Encryption
- Identity and Access Management

6.3.1.4 Server Management

To ensure servers operate as intended and do not compromise the security of computer installations or other environments.

- Servers should be configured to prevent unauthorised access or updates and to function as required.

- The configuration should disable non-essential user accounts, applications, communication services, protocols and restrict access to powerful utilities, commands, and system configuration settings to trusted individuals.

- All servers must be actively managed by a competent authority and at a minimum comply with the following policies:

    - Firewall
    - Malware Protection
    - Patch Management
    - Service Password Management

- Encryption
- Identity and Access Management

6.3.1.5 Mobile Device

To ensure mobile devices do not compromise the security of information stored on them or processed by them and prevent unauthorised access to information in the event they are lost or stolen.

- The College will protect information stored or processed via mobile devices and prevent unauthorised access when lost or stolen.
- Documented configuration standards will be deployed through a management system.
- All mobile devices must use an appropriate access control mechanism (e.g. password, pin, biometric) and have a lock out time set.
- All mobile devices must be encrypted, be capable of being remotely wiped and must be appropriately protected from malware.

6.3.2 Secure Configuration

6.3.2.1 Firewall

To prevent unauthorised network traffic from gaining access to networks or leaving networks.

- The College will operate a default inbound deny policy on all firewall devices to block unauthorised inbound connections.
- Access to the management interface of the firewall will be appropriately restricted to authorised personnel.
- There will be a managed process for documenting the requests for firewall changes.
- All such requests must contain at a minimum the details of the requestor, the changes required, duration and the business need for the firewall

change.

- All firewall change requests will be subject to a review, security assessment and must be approved by a competent authority.
- To ensure existing firewall rules are appropriate there will be periodic reviews.
- There will be a documented approval process, including risk assessment and risk management process when there is a business need for an exception.

6.3.2.2 Malware Protection

To protect the organisation against malware attacks and ensure malware infections can be addressed within defined timescales.

- The College will address the malware threat by installing anti-malware software on all appropriate devices.
- The anti-malware software will be kept up to date, with signature files updated at least daily.
- Files must be scanned upon download and access.
- Web pages must be scanned when accessed through a web browser, and connections prevented to malicious websites.
- There will be a documented process, including risk assessment when there is a business need for exceptions.
- The College will utilise sandboxing technology where it is appropriate to do so.
- The College may mandate the use of application whitelisting where it is deemed necessary.

6.3.2.3 Patch Management

To address technical system and software vulnerabilities quickly and effectively in order to reduce the likelihood of vulnerabilities being exploited and serious business impact arising.

- The College will meet it's legal and contractual obligations through a software asset management process.
- The College will protect its users, services and information by only using licensed and supported software.
- Software shall be removed from devices when no longer supported or required for business function.
- All software updates must be applied in line with an approved business processes (e.g., within 14 to 30 days of vendor release).
- There will be a documented approval process, including risk assessment and risk management process when there is a business need for an exception.
- Any systems not compliant with this policy shall be removed from the network.

6.3.2.4 Identity and Access Management

To ensure that only authorised individuals gain access to business applications, systems, networks, and computing devices, that individual accountability is assured and to provide authorised users with access privileges that are sufficient to enable them to perform their duties but do not permit them to exceed their authority.

- The College will utilise an Identity and Access Management (IAM) system.
- The IAM ensures that unique account credentials are approved and created in a timely manner to allow access to information, services and locations necessary for the roles function.

- That access permissions are granted on a need only basis and removed when no longer required.
- That accounts are disabled or removed when no longer needed.
- Standard user accounts are to be assigned by default, with a documented approval process for administrative accounts.
- Administrative accounts must be used for administrative activities only.
- 2 factor authentication will be implemented where available and required.

6.3.2.5 Password Service Management

To restrict access to business applications, systems, networks and computing devices to authorised users.

- All users should be authenticated using a unique username and password before accessing College resources.
- Password should never be requested in the form of clear text (e.g. via email, http).

6.3.2.6 Encryption

To protect the confidentiality of sensitive information, preserve the integrity of critical information and confirm the identity of the originator of transactions or communications cryptographic solutions should be approved, documented and applied throughout the organisation.

- All devices must be appropriately encrypted and use authorised services to ensure the protection of information at rest and in transit.
- Encryption technologies used must be managed to ensure that they remain secure and have documented key management processes.
- There will be a documented approval process, including risk assessment and risk management process when there is a business need for an exception.

6.4 Service Lifecycle

6.4.1 Asset Management

To help support risk-based decisions regarding hardware / software, reduce the risk of information security being compromised by weaknesses in hardware / software, protect assets against loss, support development of contracts and meet compliance requirements for licensing.

- All hardware and software should be recorded in an accurate and up-to-date asset register.
- There should be regular checks for discrepancies, and these should be investigated and resolved.
- The asset register must be protected against unauthorised change and be independently reviewed.

6.4.2 Configuration Management

To ensure that changes are applied correctly and do not compromise the security of business applications, computer systems or networks.

- Changes should be tested, reviewed and be part of a documented change management process.
- The change management process covers all types of change, such as upgrades, changes to systems and networks, software, or application and to business information.
- Any request for change must:
    - Be accepted by an authorised individual.
    - Approved by an appropriate business representative.
    - Include a risk assessment.
    - Tested.
    - Include a back-out plan.
- Once the changes have been made the following must happen:

- Changes are communicated to relevant stakeholders.
- System documentation is updated to reflect changes.
- Changes are reviewed to ensure only changes that have been authorised have taken place.
- System and information reviewed to ensure that security classifications have not changed.

6.4.3 Service Delivery Lifecycle

To ensure that business applications (including those under development) meet business and information security requirements.

- Development activities should be carried out in accordance with a documented system development lifecycle methodology.

- System development activities should be performed in specialised development environments, which are isolated from the live and testing environments, and protected against unauthorised access.

- Quality assurance of key security activities should be performed during the system development lifecycle.

- Information security requirements should be documented and agreed before detailed design commences.

- Information security requirements for systems under development should be considered when designing systems.

- System build activities (including coding and package customisation) should be carried out in accordance with industry good practice; performed by individuals provided with adequate skills / tools; and inspected to identify unauthorised modifications or changes.

- Systems under development (including application software packages, system software, hardware, communications and services) should be tested in a dedicated testing area that simulates the live environment, before the system is promoted to the live environment.

- Systems under development should be subject to security testing, using a range of attack types (including vulnerability assessments, penetration testing and access control testing).

- Rigorous criteria (including security requirements) should be met before new systems are promoted into the live environment.

- New systems should be installed in the live environment in accordance with a documented installation process.

- Post-implementation reviews (including coverage of information security) should be conducted for all new systems.

6.4.4 Compliance

To comply with laws and regulations affecting information security.

- The College recognises the critical importance of compliance and will establish a process to identify, interpret and comply with all relevant laws and regulations affecting information security. This will cover:

    - Information security-specific legislation.
    - General legislation which has security implications.
    - Regulations.
    - Contracts.

- The compliance process should be documented, signed off by executive management, and kept up to date.

- Compliance will be regularly reviewed by key stakeholders from across the College.

6.4.5 Disposal

To ensure the secure disposal of information assets and comply with legal, regulatory, and contractual obligations.

- When Technology assets have reached the end of their useful life they should be securely disposed of.
- Asset management processes must be updated with the final disposition of the technology asset's media and hardware.
- All storage mediums will be securely erased in accordance with current industry best practices.
- Approved third-party disposal service must render all data / information unreadable and provide a certificate of destruction. These certificates must be retained, and asset registers updated with the locations of the certificates.
- No computer equipment should be disposed of via skips, dumps, landfill etc.

6.5 Detection

6.5.1 Monitoring

To assess the performance of business applications, computer systems and networks, reduce the likelihood of system overload and detect potential or actual malicious intrusions.

- The College has legal, regulatory, and operational requirements to monitor activity across its network and systems.
- Information relating to this monitoring (e.g., logs) should be retained long enough to meet these requirements.
- All monitoring activities must be authorised, and regularly performed to help identify suspicious or unauthorised activity.
- All personnel authorised to perform monitoring functions must do so in accordance with the relevant ethics, procedures and safeguards.
- Monitoring activities include scanning systems for known vulnerabilities, this activity must be restricted to authorised individuals and the results presented to the system owners.

6.5.2 Logging

To help in the identification of threats that may lead to an information security incident, maintain the integrity of important security-related information and support forensic investigations.

- The College will protect the integrity of its information and systems by gathering security logs to help identify threats and support investigations.
- All systems will be assessed and configured to log appropriate security event information (e.g., failed login attempts), and the logs should be protected against unauthorised access and accidental or deliberate modification.
- Security logs should be analysed/reviewed regularly, and log retention schedules are to be defined for each system.

6.6 Response and Recovery

6.6.1 Incident Response

To identify and resolve information security incidents quickly and effectively, minimise their business impact and reduce the risk of similar incidents occurring.

- The College will identify, respond to and recover from security incidents to minimise the business impact and reduce the risk of similar incidents occurring.
- The incident response team is responsible for managing information security incidents.
- A review will take place after each incident to identify the root cause and highlight any improvements that can be made to the process.

6.6.2 Business Continuity

To provide relevant individuals with a documented set of actions to perform in the event of a disaster or emergency affecting business applications and technical

infrastructure, enabling critical business processes to be resumed within critical timescales.

- Business continuity plans should be documented for each service, provide a set of actions to perform when enacted and should be the result of a risk assessment.
- Each plan should be prepared by or in conjunction with the service owner and relate to likely scenarios.
- Roles and responsibilities should be defined and documentation/training available.
- Business continuity plans should be reviewed and tested on a regular basis.

6.6.3 Disaster Recovery

To enable critical business processes to be resumed to an agreed level, within an agreed time following a disruption, using alternative processing facilities.

- Disaster recovery plans should be documented for each critical business process to ensure they can be resumed using alternative facilities to an agreed level and timeframe.
- Alternative facilities must be ready for immediate use.

6.6.4 Backups

To ensure that, in the event of an emergency, essential information or software can be restored within critical timescales.

- Critical business information and software require a backup schedule to ensure restoration can occur within an agreed time.

- Backups should be protected from loss, damage, unauthorised access and subject to the same level of protection as the live information e.g., encrypted.

- Backups should be regularly verified by successfully testing restoration.

- The type of backup should be identified as:

Backup Type	Recovery Time	Method
Online storage	Instantaneous	Direct Attached Storage (DAS), Storage Area Network (SAN)
Near-line storage	Minutes	Automated tape library
Off-line storage	Hours	Manual IT staff restoration

6.7 External Partnerships

6.7.1 Third Party

To protect critical and sensitive information when being handled by external suppliers or when being transmitted between the organisation and the supplier.

- To protect College information when being transmitted between or handled by an external third party, information security requirements need to be considered at all stages of the relationship.

- All third parties should be identified and recorded in a register which assigns a business owner, security contact and is categorised High, Medium, Low in terms of information security.

- All third parties should agree a baseline of security arrangements for any information held, and specialised controls put in place which meet business and security needs as a result of a risk assessment.

- Termination of third-party relationships should ensure the revocation of physical and logical access, and the return or secure destruction of

information assets.

- A Business Continuity Plan (BCP) may also be required depending on the nature of the third-party service.

6.7.2 Cloud

To help ensure cloud specific risks are reduced to a level acceptable by the organisation.

- Any purchase or use of a cloud service must align with strategic goals, be centrally registered, approved, regularly reviewed and supported by a contract.

- There must be a risk assessment performed for the full lifecycle of the service including creation, processing, storage, transmissions and destruction of information.

- The risk assessment should also take into consideration the classification of data assigned and its suitability for use in the cloud.

7. Policy Statement

The Dumfries and Galloway College ("The College") ICT policy has a structure which logically groups Core, User and Management sections. This is to ensure that the relevant sections are read and understood.

The Core section must be read and adhered to by all persons involved with College ICT systems and information.

The User section must be read and adhered to by all users of the Colleges systems and data.

The Management section must be read and adhered to by any individual or entity managing a device connected to the College network or service for or on behalf of the College.

The ICT Security Policy statements are high level strategic statements written with the following principles.

- They are needed by the College.
- They clearly define the desired maturity level.
- They are achievable.
- They are measurable.

All **processes** created must conform to these policy statements.

All **procedures** created must conform to any agreed process.

All **processes** and **procedures** must also conform to all applicable organisational standards.

Guidance may also be provided to ensure that any procedure and process is competed in line with current best practice.

8. Distribution

All Staff
Repository

9. Revision Log

Revision Log		
Date	Section	Description
12.11.2020	Front page	Change of job title from Vice Principal Corporate Services and Governance to Head of Corporate Services
12.11.2020	Throughout the Policy Document	Revision to whole Policy document to reflect changes to D & G College management, security and protection of its ICT systems and data
December 2021	7 - Distribution	Changed Quality Manual to Repository
21.01.2023	Responsibility	Change of job title from Head of Corporate Services to Vice Principal People and Transformation
10.02.2023	6 - Procedure	Added USB Guidance.
10.02.2023	Throughout the Policy Document	Numbering revised.
11.05.23	Appendix 1	Equality Impact Assessment added as Appendix 1 as per revised Document Control Procedure.

Document Name	Document Owner	Revision Number	Date of Issue	Date of Withdraw
ICT Security Policy	Head of Corporate Services	1	12.11.20	
ICT Security Policy	Vice Principal People and Transformation	2		

Appendix 1: Equality Impact Assessment

Document:	ICT Security Policy
Executive Summary:	The purpose of the ICT Security policy is to minimise operational and reputational damage by reducing the impact of IT security incidents and ensure business continuity. DGC uses a large amount of information in order to operate effectively and most of this information is in digital format and held in IT systems. It is essential that this information is managed effectively so that it remains secure, accessible to authorised users and its integrity is protected. This includes providing guidance to staff to strengthen passwords and multi-factor authentication. The ICT Security Policy sets standards outlining the way digital information and IT systems should be managed and operated to ensure the DGC complies with its obligations in relation to IT Security.

Duties:

1: Eliminate discrimination, harassment and victimisation

2: Promote equality of opportunity

3: Promote good relations

* Human Rights to privacy and family life, freedom of thought and conscience, education, employment

PSED Impacts

	Commentary
Age	The policy will have a neutral impact for these characteristics.
Disability	
Gender	
Gender Based Violence	

Gender identity/ reassignment	
Marriage/civil partnership	
Pregnancy/maternity	
Religion or Belief	
Race	
Sexual Orientation	

Additional Considerations

Care experienced	The policy will have a neutral impact for these characteristics.
Carers	
Mental Health	
Socio-economic status	
Veterans	
Human Rights*	The policy will have a neutral impact on Human Rights

Lead Officer:	Vice Principal, People and Transformation		
Facilitator:	ICT Manager		
Date initiated:	06.06.23		
Consultation:			
Research:			
Signature	*Calum Rodgers*	Date	28.08.23

DUMFRIES & GALLOWAY COLLEGE

MEETING	Finance & General Purposes Committee
Agenda Item:	**7**
Paper No:	**FGP0923-7.2**

Date	13/09/2023
Location	MS Teams On-line
Title of Paper	Information Governance Group Update
Presented By	Calum Rodgers / Joe McGraw
Recommendation	**Discussion**
Appendix Attached	NO
Disclosable Under FOISA	YES

Read Time: 5 minutes

1. Recommendation

1.1 The Finance and General Purposes Committee are asked to discuss the contents of this paper.

2. Executive Summary

2.1 5 FOI requests all responded within the 20 day maximum.

2.2 Data Protection and Digital Information Bill at Public Bill Committee report stage.

2.3 Updated privacy notices being updated as required.

2.4 1 non-reportable Data security incident which was dealt with swiftly.

2.5 …

2.6 Events for Cyber Awareness Month in October 2023 are being planned.

3. Context

3.1 Freedom of Information Requests

3.1.1 5 FOI requests received since May 2023. FOISA Act requires that requests must be responded to within 20 working day and all College responses met that requirement.

3.1.2 The quarterly survey from the Scottish Information Commissioner (SIC) covering all requests received from March to June 2023 was received early July and submitted for the College. The results of the survey are posted on the SIC website to allow the public to view statistics on all public body FOI requests.

3.1.3 FOI final approval for the College has been carried out by Douglas Dickson in the absence of Jill Galloway.

3.1.4 Work is commencing to build an FOI section on AdminNet to share FOI related information and guidance.

3.1.5 An FOI Policy and Procedure are being drafted and will be submitted for approval in due course.

3.2 Data Protection/GDPR

3.2.1 The Data Protection and Digital Information (No.2) Bill. This bill has been introduced to parliament and is now at Public Bill Committee report stage. The progress of the bill has slowed slightly from the intended completion of the report stage.

3.2.2 The government aims to simplify and clarify data protection compliance, especially for small and medium-sized businesses. The bill proposes changes to the UK GDPR, the Data Protection Act 2018, and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). While the bill will make changes to data protection law if passed, its contents are not overall substantially different to current data protection law.

3.3 Privacy Notices

3.3.1 Privacy notices are produced to reflect new data processing activity, are frequently updated and can be found on the College's website. The Data Protection Team, in consultation with Information Asset Owners recently conducted a review of all privacy notices which had not been updated for more than a year and made amendments to the notices as necessary. A system will be put in place to review the notices on a quarterly cycle so that the notices remain up-to-date.

3.3.2 Minor amendments were made to the following privacy notices:

- Enrolment
- Employees
- General Teaching Council Scotland

3.3.3 A new privacy notice was added to the website for the new Observation of Learning process.

3.4 Data Subject Rights Requests and Concerns

3.4.1 The Data Protection Team has not dealt with any formal Data Subject Rights Requests during the reporting period. Any concerns raised by data subjects are dealt with in a timely manner. Additional actions which can be taken to prevent further risks and issues arising are identified and actioned.

3.5 …

3.6 Staff Training

3.6.1 A training session for Estates staff was held on 25 May 2023. Further training materials are being developed for managers with LearnNet as the preferred mode of delivery. The data protection section of AdminNet is kept up-to-date with new news items and top tips for good practice on an ongoing basis.

3.7 Data Sharing Agreements

3.7.1 The Data Protection Team will be beginning a process to review the College's Data Sharing Agreements.

3.7.2 New agreements in the period were reviewed and signed off for:

- The 1000Steps partnership
- Fife College SDS Healthcare Pathway

3.8 Cyber Update

3.8.1 No incidents had been reported since the last meeting. …

3.8.2 …

3.8.3 Additional staff training around Cyber will take place annually and communications are being developed to highlight Cyber Awareness Month in October 2023 and Scottish Cyber week in February 2024.

4. Strategic Implications

4.1 This paper is linked to Strategic Priority 2 - People and Culture, and Strategic Priority 5 - Systems and Infrastructure.

5. Risk

Risk	Mitigations
Penalties or enforcement action by the ICO, reputational damage, litigation	➢ Strong data protection framework in place ➢ Technical and organisational controls ➢ Strong incident response focused on containment, mitigation and learning lessons from incidents
11 – Failure to achieve and maintain systems and operable and secure ICT	➢ Documented disaster recovery procedures. ➢ …

6. Implications

Financial	No	No direct financial implications
Legal	Yes	Compliance with UK GDPR and the Data Protection Act 2018 (DPA 2018) and the Privacy and Electronic Communications Regulation 2003 (PECR 2003).
Learning and Teaching	No	No direct Learning and Teaching implications.
Equalities	No	No direct Equalities implications.

Calum Rodgers
ICT Manager
September 2023