Dumfries and Galloway College

One step ahead

DATA PROTECTION POLICY

Responsibility: Vice Principal People and Transformation

Issue Date: 14th June 2023

Equality Impact Assessment: 6th June 2023

Version: 1

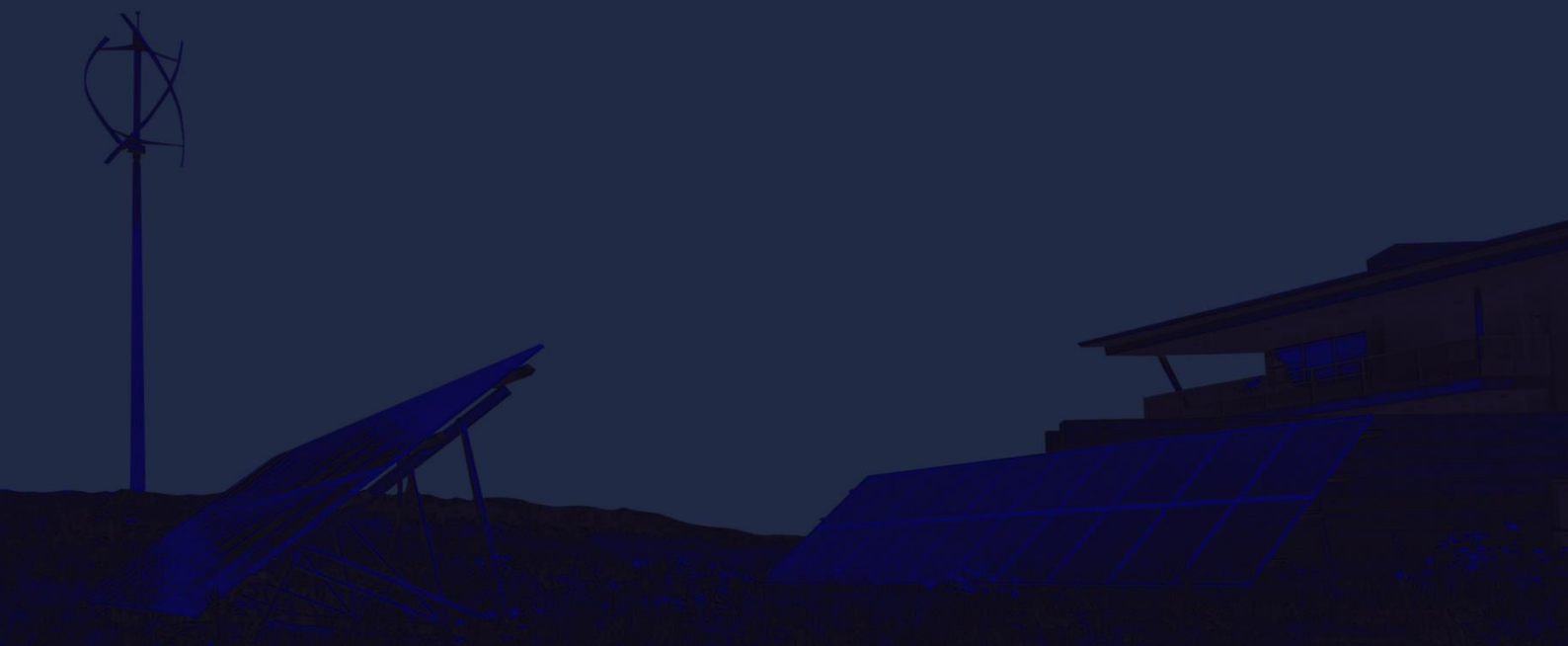

Table of Contents

Data Protection Policy

1. Purpose

In undertaking the business of Dumfries and Galloway College ("the College"), we create, gather, store and process large amounts of data on a variety of data subjects (individuals) including students (potential, current and former), staff, customers / suppliers and members of the public. This includes personal and special categories of personal data, which are subject to data protection laws.

With the ability to collect and process data comes a responsibility to ensure that this is collected, used and stored appropriately. The College must, therefore, ensure that data is managed in line with relevant legislation and guidance and that those involved in data handling and processing are aware of their responsibilities.

The College is committed to applying the principles of data protection and other requirements of data protection law to the management of all personal data at all stages of its lifecycle.

This Policy outlines how the College will fulfil its obligations as a Data Controller and where applicable, a Data Processor, under current legislative provisions for data protection, including the UK General Data Protection Regulation ("GDPR"), the Data Protection Act 2018 ("DPA 2018") and such guidance as may be issued by the UK Information Commissioner.

This policy sets out the College's data protection arrangements and ensures a common and consistent approach is adopted in relation to the management of information and the protection of personal data. This ensures:

- Information is collected, processed, held, transferred and disposed of appropriately;
- Staff are aware of their rights and responsibilities in relation to information handling;
- Appropriate mechanisms are in place to ensure that individuals whose personal information the College hold, are advised of their rights.

2. Scope

This policy applies to:

- All data created or received in the course of college business in all formats, of any age. "Data" shall include personal and special category data; and also confidential and commercially sensitive data;
- Data held or transmitted in both physical and electronic formats;

- Data transmitted in verbal format (e.g. in conversation, in a meeting, or over the telephone).

Who is affected by the policy?

- College staff (which includes contractors, temporary staff and anyone else who can access or use data, including personal and special categories of data, in their work for the college);

- Non-staff data subjects (these include, but are not confined to): prospective applicants; applicants to programmes and posts; current and former students; alumni; former employees; family members where emergency or next of kin contacts are held, members of the Board of Management and the College committees, volunteers, potential and actual donors, customers, people making requests for information or enquiries, complainants, professional contacts and representatives of funders, partners and contractors.

Where the policy applies:

This policy applies to all locations from which college data is accessed, including home use and overseas. This policy is to be implemented at all College sites and applies to all staff processing candidate, enrolled students or staff records.

3. References

- Disclosure Scotland - mygov.Scot PVG scheme
- Equality Act 2010
- Employment Rights Act 1996
- Health and Safety At Work etc. Act 1974
- Trade Union and Labour Relations (Consolidation) Act 1992
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018

4. Definitions

4.1 Special Category Data

Special Category Data is defined by UK GDPR Article 9(1):

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

The College processes Special Category Data to ensure the correct support for students and staff and to fulfil reporting obligations to governing bodies.

4.2 Criminal Conviction Data

Criminal conviction Data is data processed relating to criminal convictions and offences, or related security measures (UK GDPR, Article 10).

The most common processing of this data in the College is when staff are checked for recorded criminal convictions with Disclosure Scotland under the Protecting Vulnerable Groups (PVG) scheme. Students on work placements may also be Disclosure Scotland checked, for example, if their placement is at a nursery or requires them to work with children or vulnerable adults.

Further detail on the handling of special category and criminal convictions data can be found in Appendix 2.

5. *Responsibilities*

All users of college information (staff, students, volunteers and other users) are responsible for:

- Completing relevant training and awareness activities provided by the College to support compliance with this Data Protection Policy and other relevant policies and procedures;
- Taking all necessary steps to ensure that no breaches of information security result from their actions;
- Reporting all suspected information security (data) breaches or incidents promptly so that appropriate action can be taken to minimise harm;
- Informing the college of any change to the information that they have provided in connection with their studies or employment, for instance, changes of address or bank account details.

Data Security

- All personal data processed by the College is only accessible to those members of staff who have specific need for it in the performance of their role.
- Personal data is secured in locked filing systems within lockable rooms with controlled access where appropriate.
- Personal data which is held electronically is password protected and is subject to the College's ICT Policy Framework.
- Staff are required to keep computer passwords confidential.
- Staff should lock computers when leaving their desks.
- Staff should not leave manual records containing personal information where they can be accessed by those without authority to do so.
- Individual members of staff required to handle sensitive data in the course of their employment at the College will have a confidentiality clause contained within their written Terms and Particulars of Employment, which will explicitly state that unauthorised disclosure or a

breach of the Data Protection and Data Security Policy may result in disciplinary action.
- Access to sensitive personal data and personal data of College staff is strictly controlled and held in a secure area to which access is restricted. Similar arrangements are in place for learners' personal data where it is held within faculties or corporate services such as Student Funding or Information Systems.

Clear Desk Arrangements

The College encourages a 'clear desk' approach for those involved in handling personal data in the course of their duties. All staff with access to personal data should ensure that when work areas are unattended, no personal data or sensitive information is left unsecured.

The Principal of the College has ultimate accountability for the College's compliance with data protection law and for ensuring that the Data Protection Officer (DPO) is given sufficient autonomy and resources to carry out their tasks effectively.

The Vice Principal People and Transformation is responsible for:

- Acting as the contact for the Executive Team and ensuring that the College and staff comply with Data Protection legislation;
- Reporting to the Principal, the Audit Committee, Board of Management, and Executive Team on relevant risks and issues;
- Maintaining relevant HR policies and procedures to support compliance with data protection law;
- Ensuring that staff roles and responsibilities are clearly defined in terms of data protection and that staff contracts reflect this.

Directors within the College are responsible for:

- Ensuring all systems, processes and procedures under their remit are compliant with data protection laws
- Ensuring controls are in place and are maintained in the protection of data
- Promoting good practice in data protection among staff

- Working with the DPO and senior managers to develop and implement appropriate data protection policies and procedures.

The Data Protection Officer (DPO) is responsible for:

- Informing and advising senior managers and all members of the college community of their obligations under data protection law;
- Promoting a culture of data protection, e.g. through supporting training and awareness activities;
- Reviewing and recommending policies, procedures, standards, and controls to maintain and demonstrate compliance with data protection law and embed privacy by design and default across the College;
- Advising on data protection impact assessment and monitoring its performance;
- Monitoring and reporting on compliance to the Executive Team, the Board of Management and committees as appropriate;
- Ensuring that Records of Processing and Third party sharing activities are maintained;
- Providing a point of contact for data subjects with regard to all issues related to their rights under data protection law;
- Monitoring personal data breaches, and recommending actions to reduce their impact and likelihood of recurrence;
- Acting as the contact point for and cooperating with the Information Commissioner's Office (ICO) on issues relating to processing.

Where permissible under the legislation, some of these duties may also be undertaken by the designated College Officer with operational responsibility for data protection.

All Managers are responsible for:

- Promoting a culture of data protection compliance across the College and within their area of responsibility;
- Implementing the policy in their Faculty or Service, and for adherence by their staff;
- Ensuring that those processing data in their roles are supported in doing so appropriately.

- All Managers are responsible for implementing this policy within their business areas for adherence by staff. This includes:

- Assigning generic and specific responsibilities for data protection management;
- Managing access rights for information assets and systems to ensure that staff, contractors and agents have access only to such personal data is necessary for them to fulfil their duties;
- Ensuring that all staff in their areas of responsibility undertake relevant and appropriate training and are aware of their responsibilities for data protection;
- Ensuring that staff responsible for any locally managed IT services liaise with college's IT staff to put in place equivalent IT security controls;
- Assisting the designated College Officer with operational responsibility for data protection, and the DPO, in maintaining accurate and up to date records of data processing activities;
- Ensuring that they and their staff cooperate and support the designated College Officer with operational responsibility for data protection, and the DPO, in relation to subject access requests and other requests relating to personal data where the data is managed by their business area;
- Recording data protection and information security risks on the Organisational Risk Register and escalating these as necessary.

As part of the College's internal audit programme, the Audit Committee will instruct the College's Internal Auditors to audit the management of personal information, data protection risks and the College's compliance with relevant data protection laws.

6. Data Protection Principles

Under data protection laws the College is responsible for, and must be able to demonstrate, compliance with the six data protection principles under UK GDPR.

The College will ensure that all data processing for which it is responsible is conducted in line with these principles and this policy documents how this will be achieved in practice.

Principle 1: Personal data shall be processed fairly, lawfully and transparently

This means that the College will:

- Only collect and use personal data in accordance when we have a lawful basis to do so (see section 7 below on Lawful Basis for Processing);
- Treat people fairly by using their personal data for specific purposes and in a way that they would reasonably expect;
- Rely on consent, as the legal basis for processing, only where we obtain specific, informed and freely given consent, that is affirmative and documented; and can be easily withdrawn at any time.

Principle 2: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; (‘purpose limitation’).

This means that the College will:

- ensure that if we collect personal data for one purpose (e.g. to provide advice on study skills), we will not reuse this data for a different purpose that the individual did not agree to or expect (e.g. to promote goods and services for an external supplier);
- inform data subjects about the specific purposes of processing and tell them what we are doing with their personal data.

Principle 3: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’).

This means that the College will:

- Only collect personal information where it is necessary so that we can deliver our functions and services;
- Reduce risks of disclosure by anonymising personal data wherever necessary, (e.g. when using it for statistical purposes), so that individuals can no longer be identified;
- Review the data we hold and where appropriate delete what we do not need.

Principle 4: **Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').**

This means that the College will:

- Take all reasonable steps to ensure the personal data we hold is accurate and record the source of that data (e.g. from data subject or partner organisation);
- Have processes in place to ensure that incorrect data is rectified or erased as soon as possible;
- Update personal data where appropriate, (e.g. when informed of a change of address our records will be updated accordingly).

Principle 5: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; ('storage limitation').

This means that the College will:

- Only keep personal data for as long as necessary for the purpose it was collected for; and destroy records securely in a manner appropriate to their format;
- Apply agreed retention periods to all records containing personal data;
- Have appropriate processes in place to comply with individuals' requests for erasure under the 'right to be forgotten'.

Principle 6: Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

This means that the College will:

- Have robust organisational measures in place to protect personal data, including physical and technical security measures (e.g. secure rooms and storage where appropriate, an ICT Security Policy and ICT Acceptable Use Policy;
- Control access to personal data so that staff, contractors and other people working in the College can only see the personal data that is necessary for them to fulfil their duties;
- Require all College staff, contractors, students and others who have access to personal data in the course of their work to complete data protection training, supplemented as appropriate by procedures and guidance relevant to their specific roles;
- Implement a Data Breach Procedure to manage, investigate and, where applicable, report security incidents to the ICO and data subjects affected.

The Accountability Principle

Accountability is central to UK GDPR. The College must take responsibility for what it does with personal data and how it complies with the above principles. The College is required to maintain necessary documentation of all processing activities; implement appropriate security measures (technical and organisational); perform Data Protection Impact Assessments (DPIAs) and designate a DPO.

7. *Lawful Basis For Processing*

To be able to process data lawfully, the College must ensure that all processing falls within one or more of the lawful bases (conditions for processing) as set out in Article 6 of the GDPR. These are:

- **Consent** – An individual has provided clear consent for the processing of their personal data for one or more specified purposes;
- **Contract** – The processing of the personal data is necessary to fulfil a contract that the College has with an individual;
- **Legal Obligation** – Processing of data is necessary to comply with the law, other than to fulfil a contractual reason;
- **Vital Interests** – Processing of data is necessary to protect someone's life;
- **Public Task** – Processing is necessary for the College to perform a public interest task or to fulfil its official functions, where the task or function has a clear legal basis;
- **Legitimate Interests** – Processing is necessary for the College's legitimate interests or the legitimate interests of a third party, unless the need to protect an individual's personal data overrides those legitimate interests.

At each point that the College collects data, the lawful basis for processing will be made clear.

8. *Privacy Notices*

The College will use privacy notices to let data subjects know what is done with their personal data. The text of all privacy notices will be consistent across the College and will confirm what the lawful basis is for the processing of the data.

Privacy notices are published on the college website and are made available to individuals from their first point of contact with the College.

Any processing of staff or student data beyond the scope of the standard privacy notices will mean that a separate privacy notice is required.

We will regularly review these privacy notices and will inform the data subjects of any changes that may affect them.

9. Data Subjects Rights and Subject Access Requests

Data subjects have the following rights under data protection law:

The right to be informed,
The right of access,
The right to rectification,
The right to erasure,
The right to restrict processing,
The right to data portability,
The right to object,
Rights in relation to automated decision making and profiling.

These rights are explained in further detail in the Data Subject Rights Procedure. The College will uphold Data Subject Rights (DSRs) and have appropriate processes and procedures in place to ensure these rights can be actioned if an individual makes a request. It is important to note that some rights have certain conditions that must be met for the rights to apply.

Individuals always have the right to request access to their personal data that the College holds (known as making a Subject Access Request (SAR). Any data subject may make such a request and receive a copy of their information usually free of charge and within one month of their request. For further details see 'Guide - How to make a Subject Access Request' and 'Subject Access Request Procedure'.

When an individual makes any request to exercise any of their rights then the designated College Officer with operational responsibility for data protection must be informed immediately, so this can be recorded and processed accordingly. **All requests must be answered within one month.**

The College will maintain a central DSR Register to demonstrate for audit and reporting purposes that we are meeting the deadlines for handling all requests. The DSR Register will be held securely by the designated College Officer with operational responsibility for data protection.

The College will also ensure it communicates to all data subjects their right to lodge a complaint with the ICO.

10. Data Protection Impact Assessment (DPIAs)

Where the College proposes to introduce or amend new systems or working practices that have implications for its data protection arrangements, a DPIA will be completed to assess these implications, manage risk and to consider what control measures are appropriate to ensure that data remains protected, and all processing remains compliant with the principles set out above.

Where any relevant new project or system is being considered the DPO must be advised at the earliest opportunity in order that they can consider the proposal and determine whether a DPIA is required. For further information please contact the DPO via the data protection mailbox dpo@dumgal.ac.uk.

11. Staff Training

The College will provide initial data protection training for all staff (existing and new), with additional specialist training given to staff in areas with specific responsibilities for processing personal data and sensitive information. Periodic refresher training will be given to all staff.

Completion of initial and refresher training in data protection will be mandatory for all College staff.

12. Data Sharing

In the performance of its duties in relation to the employment of staff and the services provided to learners, the College is required to share information with external organisations. Example bodies with whom the College may be required to share or give access to data include:

Scottish Government	Scottish Funding Council
Awarding Bodies	Education Scotland
Skills Development Scotland	HMRC
Pension Funds	Trades Unions
Local Authorities	Insurance Companies
Legal Advisers	Scottish Public Services Ombudsman
Auditors	Suppliers of services, such as College systems
General Teaching Council Scotland (GTCS)	

In all such cases where personal data is shared externally, the College will ensure that appropriate safeguards are in place through agreed protocols or data sharing agreements by College Officer with operational responsibility for data protection.

12.1 Transfer of Data/Information Cross Campus

College staff may only share the personal data we hold with another member of staff if the recipient specifically needs to know it for a job/task. Most data processed by the College is available via relevant College systems at any campus to those who require access and there should be no need for such data to be transferred by staff using portable means. (For further information about the use of USBs, portable hard drives and the transfer of manual files see Data Security and the ICT Security Policy)

12.2 Data Sharing with the Police and Statutory Agencies

There is a particular exemption within the data protection legislation relating to requests for access to personal information received from the police, law

enforcement agencies and other bodies with statutory functions to detect or prevent crime. Such requests should normally be made in writing and signed by someone of sufficient authority within the agency requiring the information.

If you receive a request from such an agency, you must consult with a member of the Executive Management Team who will make the decision whether personal information should be released.

12.3 Disclosure of data to third parties

The College must ensure that personal data is not disclosed to unauthorised third parties which includes family members. All staff and students should exercise caution when asked to disclose personal data held about an individual to a third party. Disclosure must be relevant to, and necessary for, the conduct of College business or under legal obligation.

Requests for information in relation to an individual will only be accepted if produced in writing, on company-headed paper. The reason for making the request and, where appropriate, the legal basis for the request must be detailed. Where appropriate, a statement from the data subject consenting to disclosure to the third party should accompany the request.

If there is any doubt as to whether it is legitimate to disclose personal information to a third party, staff should seek advice from their line manager who will consult with the designated College Officer with operational responsibility for data protection, a member of the Executive Management Team, or the DPO as necessary.

13. Data Security

The following general principles apply at all times to all data managed by the College, whether the data are personal and/or special category data; confidential business data; or commercially sensitive data:

- All college users of data must ensure that all data, and specifically personal and special category data, they hold is kept securely;
- Users must ensure data is not disclosed to any unauthorised third party in any form either accidentally or otherwise (including verbal disclosure);
- Desks should be left clear at the end of each working day; paperwork shall be locked away when not in use;
- Portable devices (laptops, memory sticks, external hard drives) should not be left unattended.
- For further information see ICT Security Policy/ICT Acceptable use Policy

14. Data Retention and Disposal

The College will develop a College wide Data Retention Schedule**.** This sets out the basis on which information can be retained and documents retention periods; as set out in legislation or in line with record keeping requirements set by relevant statutory bodies.

Personal data must only be kept for the specified retention period. Once information is no longer needed it should be disposed of securely.

The College has appropriate measures in place for the deletion and disposal of personal data. Manual records are shredded and disposed of as "confidential waste" and arrangements are in place to permanently erase the hard drives of redundant electronic equipment.

15. Data Breaches

While the purpose of this policy is to ensure that the College's data protection arrangements are effective and well understood, it is also important to recognise the behaviours and actions that would be considered as breaches of the policy and the consequences of any such breach. The following occurrences are considered breaches of this policy:

- Unlawful procurement of information by anyone not entitled to access such information;
- Unfair processing i.e. processing information for a purpose other than that for which it was provided or consent was given;
- Processing of inaccurate information, particularly if information was known to be inaccurate or steps could have been taken to ensure accuracy;
- Unlawful disclosure i.e. sharing of information with anyone not entitled to receive it or loss of any data covered in this policy;
- Collection, storage or processing of inadequate, irrelevant or excessive information.

The College will take all necessary steps to reduce the likelihood of Personal Data Breaches and to reduce the impact of any incidents involving personal data that do occur.

In line with the College's Data Breach Procedure all personal data breaches (suspected and actual) must be reported your Line Manager and the designated College Officer with operational responsibility for data protection immediately. If a breach is likely to result in a risk to the rights and freedoms of an individual, the DPO must be informed as the College is required to report to the ICO within 72 hours of notification.

The College will record all data incidents and reportable breaches. We will use these events as 'learning points' as part of the continual improvement of our data handling processes.

The College is committed to a culture which encourages early identification of personal data incidents and which provides appropriate training and support to individuals involved. However, the College will, where deliberate or wilful behaviour leads to a data protection incident, take appropriate disciplinary action and/or report the matter to the police, in line with relevant HR policies.

16. Risks of non-compliance

The penalties for a breach of the GDPR are significant. This may include penalties of up to £17,500,000 or 4% of annual turnover (whichever is greater) for the most serious breaches of the law; plus claims for compensation and damage to reputation.

Misuse of personal data, through loss, disclosure or failure to comply with the data protection principles and the rights of data subjects, may result in significant legal, financial and reputational damage for the College.

Non-compliance with the data protection principles, or any concerns over data protection, must immediately be reported to dpo@dumgal.ac.uk and to your Line Manager.

17. Monitoring and review

The College will review its practices and guidance on a regular basis to ensure that they reflect our commitment to ensuring fair, consistent and lawful management of data. This policy will be reviewed every three years to reflect legislative requirements, recommendations and identified good practice.

18. Linked Policies/Related Documents

This policy should be read in conjunction with the College's:

- Special Category and Criminal Convictions Data Policy
- ICT Security Policy
- ICT Acceptable Use Policy
- Data Breach Procedure
- Data Subject Request Procedure
- Disciplinary Policies and Procedures
- SQA – Systems verification

19. Distribution

All Staff
Repository

20. Revision Log

Revision Log		
Date	Section	Description
December 2021	19 – Distribution	Quality Manual changed to Repository
01.04.22	Responsibility (Front Cover) and 5.	Changed from Vice Principal Business Development and Corporate Services to Vice Principal People and Transformation
01.04.22	Responsibility 5.	Job titles changed to reflect change in organisational structure
01.04.22	12.2	Executive Management Team changed to Executive Leadership Team
02.03.23	1 and 16	EU GDPR changed to UK GDPR; removal of reference to euros
16.03.23	Minor changes throughout Appendix Added	Alignment with Quality template headings Special Category & Criminal Convictions Policy incorporated as Appendix
06.06.23	Appendix 1	Equality Impact Assessment added as Appendix 1

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
Data Protection Policy	Vice Principal People and Transformation	1	14.06.23	

Appendix 1 – Equality Impact Assessment

Document:	Data Protection Policy
Executive Summary:	The ability to control availability of data held should ensure that personal equalities profile data is securely held and used only for appropriate purposes, reducing discrimination across all protected characteristics. The Policy supports human rights detailed in the European Convention on Human Rights and Human Rights Act 1998. This policy should ensure that individuals trust us to collect and hold their information, improving our systems for rooting out and addressing indirect discrimination and for assessing progress in terms of equality. Discrimination will be prevented by maintaining high levels of confidentiality around personal characteristics, equality of opportunity will be promoted through the rooting out of indirect discrimination via the analysis of data provided due to the effectiveness of this 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	Promotes duties 1, 2, and 3 above
Disability	
Gender	
Gender Based Violence	Promotes duties 1, 2, and 3 above. This policy should ensure that individuals trust us to collect and hold their information where they access support or report issues in connection with safeguarding. This policy complements

	the College's existing framework of safeguarding procedures.
Gender identity/ reassignment	Promotes duties 1, 2, and 3 above.
Marriage/civil partnership	
Pregnancy/maternity	
Religion or Belief	
Race	
Sexual Orientation	

Additional Considerations

Care experienced	Promotes duties 1, 2, and 3 above
Carers	
Mental Health	
Socio-economic status	
Veterans	
Human Rights*	The Human Rights to Education, Employment and Privacy are positively progressed by this policy.

Lead Officer:	Douglas Dickson (obo Jill Galloway)		
Facilitator:	Jennie Griffiths		
Date initiated:	06/06/2023		
Consultation:	UK GDPR forms the basis of our policy.		
Research:			
Signature	Jill Galloway	Date	06/06/23

Appendix 2– Special Category & Criminal Convictions Policy

SPECIAL CATEGORY AND CRIMINAL CONVICTIONS DATA POLICY

1. Purpose

As an employer, and in the provision of education under our public tasks, we process special category data and criminal offence data. The purpose of this policy is to outline Dumfries & Galloway College's ("the College") approach to the management of special category and criminal conviction data processed by the College.

Data protection law requires controllers who process special category or personal data relating to criminal convictions and offences under various parts of the Data Protection Act 2018 to have an "appropriate policy document" in place setting out additional safeguards for the processing of this data.

This policy sits as Appendix 1 to the core Data Protection Policy created and maintained by the College.

2. Scope

This policy document applies to all staff employed by the College and its provisions extend to all special category personal data and criminal convictions data we process (or a third party processes on our behalf).

3. References

- Disclosure Scotland - mygov.Scot PVG scheme
- Equality Act 2010

- Employment Rights Act 1996
- Health and Safety At Work etc. Act 1974
- Trade Union and Labour Relations (Consolidation) Act 1992
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018

4. Definitions

For the purposes of this policy, the following definitions apply:

Criminal conviction data

Data processed relating to criminal convictions and offences, or related security measures (UK GDPR, Article 10).

The most common processing of this data in the College is when staff are checked for recorded criminal convictions with Disclosure Scotland under the Protecting Vulnerable Groups (PVG) scheme. Students on work placements may also be Disclosure Scotland checked, for example, if their placement is at a nursery or requires them to work with children or vulnerable adults.

Special category data

Defined by UK GDPR Article 9(1):

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

The College processes Special Category Data to ensure the correct support for students and staff and to fulfil obligations to governing bodies.

Record of Processing Activities (RoPA)

Under Article 30 UK GDPR, the College is required to maintain a record of processing activities under its' responsibility. The ROPA details all data processing activities across the College and includes details of the processing, retention and erasure of special category and criminal convictions personal data.

5. Responsibilities

This Policy applies to all College staff and contractors processing special category and criminal convictions data.

5.1 Staff Training

The College will ensure all staff are trained in data protection, specifically relating to personal, special category, and criminal data and the legislation underpinning this. This training will be periodically refreshed and will form part of the induction process for all new staff.

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

Staff should, in the first instance, discuss their query with their line manager. If their line manager is unavailable or further assistance is required, they should contact the Data Protection Team on DPO@dumgal.ac.uk .

5.2 How will we know if this policy is working?

The College will monitor compliance with this policy by keeping its RoPA up-to-date and monitoring changes in practice or in legislation.

Statistics and anonymous information may be provided to senior management and auditors based on the content of the RoPA.

Through staff training and ongoing support provided by the Data Protection Team, the College will maintain data protection policy and procedure awareness.

6. Special Category Data

Special category staff and students data will be processed by the College for a number of reasons related to the specified purpose for which it was originally collected.

Staff Data (Including Board of Management)	
Purpose of Processing	Lawful Basis
Sickness Absence	• UK GDPR Article 6(1)(b) - performance of a contract • UK GDPR Article 9(2)(g) – reasons of substantial public interest • DPA 2018, Schedule 1, Part 1, 2. Health and Social care purposes (b) assessment of the working capacity of an employee (*Employment Rights Act 1996*)
Occupational health	• UK GDPR Article 6(1)(b) – performance of a contract • UK GDPR Article 9(2)(h) – occupational medicine and assessment of working capacity of an employee • UK GDPR Article 9(2)(g) – reasons of substantial public interest • DPA 2018, Schedule 1, Part 1, 2. Health and Social Care purposes (a) occupational medicine and (b) assessment of working capacity of an employee. (Health and Safety at Work etc. Act 1974)
Counselling services	• UK GDPR Article 6(1)(b) – performance of a contract • UK GDPR Article 9(2)(g)- reasons of substantial public interest • DPA 2018, Schedule 1, Part 2, 17 – counselling etc (Health and Safety at Work etc. Act 1974)

Disciplinary and grievance procedures	• UK GDPR Article 6(1)(b) – performance of a contract • UK GDPR Article 9(2)(b) – employment law • UK GDPR Article 9(2)(g) – reasons of substantial public interest • DPA 2018, Schedule 1, Part 2, 11 protecting the public against dishonesty etc. (2)(a) – protect members of the public against dishonesty, malpractice, or other seriously improper conduct (Employment Rights Act 1996)

Staff Data (Including Board of Management)	
Purpose of Processing	**Lawful Basis**
Trade Union membership data	• UK GDPR Article 6(1)(b) – performance of a contract • UK GDPR Article 9(2)(b) – employment and social protection law • UK GDPR Article 9(2)(g) – reasons of substantial public interest • DPA 2018, Schedule 1, Part 2, 6. (2)(a) – exercise of a function conferred by an enactment or rule of law (Trade Union and Labour Relations (Consolidation) Act 1992)
Equality and diversity data	• UK GDPR Article 6(1)(e) – performance of task in the public interest • UK GDPR Article 9(2)(g) – reasons of substantial public interest • DPA 2018, Schedule 1, Part 2, 8. (1) – equality or opportunity of treatment (Equality Act 2010)
Protected Disclosures	• UK GDPR Article 6(1)(e) – performance of task in the public interest • UK GDPR Article 9(2)(g) – reasons of substantial public interest • DPA 2018, Schedule 1, Part 2, 6. (2)(a) – exercise of a function conferred by an enactment or rule of law (Employment Rights Act 1996, Public Interest Disclosure Act 1998)
Safeguarding	• UK GDPR Article 6(1)(c) legal obligation • UK GDPR Article 9(2)(g) reasons of substantial public interest

	• DPA 2018, Schedule 1, Part 2, (18) Safeguarding of children and of individuals at risk • Children and Young People (Scotland) Act 2014, Part 9 Corporate Parenting provisions.

Student Data	
Purpose of Processing	Lawful Basis
Equality and diversity data	• UK GDPR Article 6(1)(e) – performance of task in the public interest • UK GDPR Article 9(2)(g) – reasons of substantial public interest • DPA 2018, Schedule 1, Part 2, 8. (1) – equality or opportunity of treatment (Equality Act 2010) • DPA 2018, Schedule 1, Part 2, 6. (2)(a) – exercise of a function conferred by an enactment or rule of law (Equality Act 2010)
Counselling services	• UK GDPR Article 6(1)(b) – contract • UK GDPR Article 9(2)(g)- reasons of substantial public interest • DPA 2018, Sch 1, Part 2, 17 – counselling etc (Health and Safety at Work etc. Act 1974)
Personal learning support plans	• UK GDPR Article 6(1)(e) – performance of task in the public interest • UK GDPR Article 9(2)(g) - reasons of substantial public interest • DPA 2018, Sch 1, Part 2, 16 – support for individuals with a particular disability or medical condition (Equality Act 2010)
Personal escape plans	• UK GDPR Article 6(1)(e) – performance of task in the public interest • UK GDPR Article 9(2)(g) - reasons of substantial public interest • DPA 2018, Sch 1, Part 2, 16 – support for individuals with a particular disability or medical condition (Equality Act 2010)
Safeguarding	• UK GDPR Article 6(1)(c) legal obligation

	• UK GDPR Article 9(2)(g) reasons of substantial public interest • DPA 2018, Schedule 1, Part 2, (18) Safeguarding of children and of individuals at risk • Children and Young People (Scotland) Act 2014, Part 9 Corporate Parenting provisions.

7. Criminal Convictions Data

The College has a statutory duty to protect children and vulnerable adults, as outlined in the Protection of Vulnerable Groups (Scotland) Act 2007. Under this legislation, the College will conduct criminal convictions checks to ensure that its staff do not pose a threat to the safety of children and vulnerable adults.

Similarly, the College will conduct criminal convictions checks to ensure that students undertaking regulated work with children and/or vulnerable adults do not pose a threat to their safety.

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

UK GDPR Article 6(1)(c) – legal obligation
UK GDPR Article 9(2)(g) – reasons of substantial public interest
DPA 2018, Schedule 1, part 2, 18 – safeguarding of children and individuals at risk (Protection of Vulnerable Groups (Scotland) Act 2007)

8. Distribution

All Staff
Repository

9. *Revision Log*

Revision Log		
Date	Section	Description

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
Special Category and Criminal Convictions Data Policy	Vice Principal People and Transformation	1		

Appendix 1 – Equality Impact Assessment

Document:	Special Category and Criminal Convictions Data Policy
Executive Summary:	The ability to control availability of data held should ensure that personal equalities profile data is securely held and used only for appropriate purposes, reducing discrimination across special category data and protected characteristics. The Policy supports human rights detailed in the European Convention on Human Rights and Human Rights Act 1998.

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	General policy provisions promote duties 1, 2, and 3 above
Disability	General policy provisions promote duties 1, 2, and 3 above. This policy promotes the additional protection of special category health data.
Gender	General policy provisions promote duties 1, 2, and 3 above.
Gender Based Violence	General policy provisions promote duties 1, 2, and 3 above. This policy complements the College's existing framework of safeguarding procedures.
Gender identity/ reassignment	General policy provisions promote duties 1, 2, and 3 above. This policy promotes the additional protection of special category health data. This policy will ensure that staff are not at risk of a criminal conviction or prejudice for revelation of the gender reassignment status of an employee or student.

Marriage/civil partnership	General policy provisions promote duties 1, 2, and 3 above.
Pregnancy/maternity	General policy provisions promote duties 1, 2, and 3 above. This policy promotes the additional protection of special category health data.
Religion or Belief	General policy provisions promote duties 1, 2, and 3 above. This policy promotes the additional protection of special category data.
Race	
Sexual Orientation	

Additional Considerations

Care experienced	General policy provisions promote duties 1, 2, and 3 above.
Carers	
Mental Health	General policy provisions promote duties 1, 2, and 3 above. This policy promotes the additional protection of special category health data, including mental health data.
Socio-economic status	General policy provisions promote duties 1, 2, and 3 above.
Veterans	
Human Rights*	The Human Rights to Education, Employment and Privacy are positively progressed by the general and specific provisions in this policy

Lead Officer:	Douglas Dickson (obo Jill Galloway)		
Facilitator:	Jennie Griffiths		
Date initiated:	06/06/2023		
Consultation:	UK GDPR forms the basis of our policy.		
Research:			
Signature	Jill Galloway	Date	06/06/23