POLICY & PROCEDURE	**DATA PROTECTION POLICY**
Policy Number	
Date of first issue	**January 2019**
Reissue date	**January 2025**
Issue number	**003**
Approving committee	**Executive Leadership Team**
Date of approval	**October 2021**
Responsible person	**Vice Principal Finance and Infrastructure**
Equality Impact Assessment	**April 2021**
Review date	**January 2027**

Other Documents Policy Refers to

Document Title
ICT Security Policy
ICT Acceptable Use Policy
Data Breach Procedure
Special Category and Criminal Offence Data Policy
Data Subjects' Rights Policy
Subject Access Request Procedure
DPIA Policy
Procedure for Managing Requests for Personal Data from Police Scotland & Other Government Agencies
Third Party Authority Procedure
Staff Disciplinary Policy

All documents are available on College Connections

History of amendments

Date	Version/Pages/Sections affected	Summary of changes
October 2024	Throughout document	Updated job roles in line with current organisational structure
October 2024	Section 5	All Heads of Curriculum and Head of Services responsibilities updated to clarify this refers to responsibilities for 'data protection' and 'personal data'
October 2024	Section 8	New section added to reference the Special Category and Criminal Offences Data (Appropriate Policy Document).
October 2024	Section 9	Guide at Appendix 2 replaced with link to online ICO guidance
October 2024	Section 10	Reference included to new Data Subject Rights Policy
October 2024	Section 11	Reference included to Data Protection Impact Assessment Policy (DPIA Policy)
October 2024	Section 13	Data Sharing section specifies the requirement to monitor data sharing arrangements to ensure they are effective
October 2024	Section 13.3	This now refers to process for ad hoc requests for information and the College's Third-Party Authorisation Procedure

CONTENTS

1 INTRODUCTION

This policy outlines how Ayrshire College ("the College") will fulfil its obligations as a Controller and where applicable, a Data Processor, under current legislative provisions for data protection in the UK, and such guidance as may be issued by the UK Information Commissioner.

2 PURPOSE

The purpose and benefits of this policy are to raise awareness of the College's data protection arrangements to ensure that a common and consistent approach is adopted in relation to the management of information and the protection of personal data in order that:

- 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 holds are advised of their rights

3 POLICY STATEMENT

In undertaking the business of the College, we create, gather, store and process substantial amounts of data about a range 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.

4 SCOPE

This policy applies to:

- all data created or received during college business in all formats, of any age. "Data" shall include personal and special category data, also confidential and commercially sensitive data
- data held or transmitted in physical (including paper) 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.

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 procedures
- taking all necessary steps to ensure that no data security incidents result from their actions
- reporting all suspected data security incidents promptly so that appropriate action can be taken to minimise harm
- informing the College of any changes to the information that they have provided in connection with their studies or employment, for instance, changes of address or bank account details

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 Finance and Infrastructure is responsible for:

- reporting to the Senior Leadership Team and ensuring that the College and staff comply with Data Protection legislation
- reporting to the Principal, the Audit and Risk Committee, Board of Management, and Senior Leadership Team on relevant risks and issues
- overseeing internal data protection activities and ensuring that procedures are in place for individuals to exercise any of their rights

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

The Director of Digital Infrastructure is responsible for:

- ensuring the security of all centrally managed IT systems and services operated by the College and the protection of electronic data
- promoting good practice in IT security among staff
- ensuring that IT security risks related to data protection are captured on the College risk registers

The Head of Facilities is responsible for:

- ensuring that controls are in place to manage the physical security of the College, including CCTV, taking account of relevant data protection laws and risks

The Vice Principal People, Performance and Transformation is responsible for:

- 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

The Head of Quality Enhancement is responsible for:

- maintaining relevant student administration policies and procedures

The Head of Business Intelligence and Information Systems is responsible for:

- oversight of the management of student records and associated personal data across the College in compliance with data protection law

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
- developing appropriate data protection policies and procedures with appropriate senior managers
- reviewing and recommending policies, procedures, standards, and controls to maintain and demonstrate compliance with data protection law and embed data protection by design and default across the College
- providing advice where requested regarding data protection impact assessments and monitoring performance
- monitoring and reporting on data protection compliance to the Senior Leadership Team, the Board of Managers and committees as appropriate

- ensuring that records of processing and third-party sharing activities are maintained
- providing a point of contact for data subjects regarding all issues related to their rights under data protection law
- monitoring personal data breaches and recommending actions to reduce their impact / likelihood of recurrence
- acting as the contact point for and cooperating with the Information Commissioner's Office (ICO) on issues relating to processing

All Heads of Curriculum and Heads of Services are responsible for:

- promoting a culture of data protection compliance across the College and within their area of responsibility
- implementing this policy and related procedures in their faculty or Service, and for adherence by their staff
- having a duty of care for ensuring the security of all IT systems and services within their area(s) and the protection of personal data in all formats
- ensuring compliance with college data protection policies and procedures when planning and / or implementing new IT systems or processes involving personal data within their area
- ensuring that those processing personal data in their roles are supported in doing so appropriately

All Managers are responsible for implementing this policy within their business areas and 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 that 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 the College's IT staff to put in place equivalent IT security controls
- maintaining accurate and up to date records of data processing activities
- ensuring that they and their staff understand their responsibilities for responding to any Data Subject Requests relating to personal data that is managed by their business area
- recording data protection and information security risks on the Organisational Risk Register and escalating these as necessary

6 DATA PROTECTION PRINCIPLES

Under data protection laws the College is responsible for and must be able to demonstrate compliance with the data protection principles.

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:

- collect and use personal data only when we have a lawful basis to do so (see section 7, Lawful Basis for Processing)
- treat people fairly by using their personal data for specific purposes and in a way that they would expect
- inform individuals about how we process their personal data in Privacy Notices; these will be made available when data is collected and published on our website

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 individuals 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 from a third party)
- have processes in place to ensure that inaccurate 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 data security incidents to the ICO and to individuals affected

The Accountability Principle

Accountability is central to data protection. 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

The College must have a valid lawful basis to process personal data. There are six available lawful bases for processing.

- **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

No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on our purpose and relationship with the individual.

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

8 APPROPRIATE POLICY DOCUMENT AND ADDITIONAL SAFEGUARDS

As part of the College's statutory functions, we process special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the UK General Data Protection Regulation ('UKGDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

Some of the Schedule 1 conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document ('APD') in place. This sets out and explains our procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data.

The **Special Category and Criminal Offence Data Policy (The APD)** explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018. The APD should be read alongside this Data Protection Policy.

9 PRIVACY NOTICES

The College will provide privacy notices to let individuals know how we use their personal data. The text of all privacy notices will be consistent across the College and will include all the required information under Article 13 and 14 of the UKGDPR, such as the lawful basis for processing as well as the purposes of processing.

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.

10 DATA SUBJECTS RIGHTS AND SUBJECT ACCESS REQUESTS

Data subjects (individuals) 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

Further detail can be found on the ICO's website 'A guide to individual rights'.

The College will implement a **Data Subject Rights Policy**. This policy will ensure that the College has a robust and systematic process for responding to any data subject requests that involve personal data. 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 access and receive a copy of their personal data that the College holds. This is known as making a Subject Access Request (SAR). Any individual 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 the College's **Subject Access Request Procedure**.

When an individual makes any request to exercise any of their rights then the Information and Customer Relations Officer 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 Register of Data Subject Requests to demonstrate for audit and reporting purposes that we are meeting the deadlines for handling all requests. This Register will be held securely by the Information and Customer Relations Officer.

The College will tell individuals about their right to lodge a complaint with the ICO. We will provide contact details of the ICO in all privacy notices.

11 DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

Where the College proposes to introduce or amend new systems or working practices that have implications for its data protection arrangements, a Data Protection Impact Assessment (DPIA) Screening Form will be completed to assess these implications, manage risk and to consider what control measures are appropriate. This is to ensure that processing of personal data remains compliant with the principles set out above.

Where any relevant new project or system is being considered and this involves personal data, staff must follow the **Data Protection Impact Assessment Policy (the DPIA Policy).** This means that a DPIA Screening Form will be completed at the earliest opportunity. This will then be considered by the DPO to determine whether a full DPIA is required.

12 STAFF TRAINING

The College will provide initial (induction) 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. Regular refresher training will be available to all staff.

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

13 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

In all cases where personal data is shared externally, the College will ensure that appropriate safeguards are in place through agreed protocols or data sharing agreements. Data sharing arrangements will be monitored to ensure they are effective. The College will maintain a Register of all Data Sharing Agreements.

14.1 Transfer of personal data / Sharing of information internally

College staff may only share the personal data we hold with another member of staff if the recipient has a job-related need to know. 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 and guidance about the use of USBs, portable hard drives and the transfer of manual files staff should contact the Director of Digital Infrastructure).

14.2 Data Sharing with the Police and other 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.

Any member of staff who receives such a request must inform their Line Manager who will consult with a one of the named officers in **Procedure for Managing Requests for Personal Data from Police Scotland & Other Government Agencies**. The Data Protection Officer will offer advice as required.

14.3 Disclosure of data to third parties

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

One-off or ad hoc requests for information from organisations will only be accepted if produced in writing. The College will keep a record of any personal data shared with third parties. The College has a Template Data Sharing Request Form for this purpose. Where appropriate, a statement from the data subject authorising disclosure to the third party should accompany the request.

For one-off or ad-hoc requests for information from individuals, including parents, guardians, spouses or partners, the College will ONLY share student/staff data if the individual has provided authorisation to disclose. The College has a Third Party Disclosure Form for this purpose and a Third-Party Authority Procedure for staff, which will assist in dealing with third party requests for information.

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 a member of the Senior Leadership Team, or the DPO, as necessary.

14 DATA SECURITY

The following general principles always apply 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

15 DATA RETENTION AND DISPOSAL

The College will keep personal data for as long as it is needed to achieve specified purposes. The College's Retention Schedule documents agreed retention periods; as set out in legislation, in line with requirements set by relevant statutory bodies or according to business need. Personal data must only be kept for the specified retention period. Once information is no longer needed it will 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.

16 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
- 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 subject to this policy
- Collection, storage or processing of inadequate, irrelevant or excessive information

The College will take all necessary steps to reduce the likelihood of data security incidents 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 DPO copying in the Vice Principal, Finance and Infrastructure 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 security incidents and reportable breaches. It will use these events as 'learning points' as part of the continual improvement of College 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 security incident, take appropriate disciplinary action and/or report the matter to the Police, in line with relevant HR policies.

17 RISKS OF NON-COMPLIANCE

The penalties for infringements of data protection legislation are significant. This may include penalties of up to £17.5m or 4% of global annual turnover 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 the College's DPO dataprotection@ayrshire.ac.uk and to your Line Manager.

18 ASSOCIATED DOCUMENTS

This policy should be read in conjunction with the following College policies and procedures:

- ICT Security Policy
- ICT Acceptable Use Policy
- Data Breach Procedure
- Policy document – Special category and criminal offence data
- Data Subjects' Rights Policy
- Subject Access Request Procedure
- DPIA Policy
- Procedure for Managing Requests for Personal Data from Police Scotland & Other Government Agencies
- Third Party Authority Procedure
- Staff Disciplinary Policy

19 LEGISLATION

18.1 Legislation relevant to this policy includes:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018

20 POLICY 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.

21 DISTRIBUTION

- All Staff
- Published on College Connections
- Published on College website