POLICY & PROCEDURE	**DATA PROTECTION POLICY**
Policy Number	
Date of first issue	**January 2019**
Reissue date	
Issue number	**002**
Approving committee	**Executive Leadership Team**
Date of approval	**October 2021**
Responsible person	**Assistant Principal, Finance, Student Funding and Estates**
Equality Impact Assessment	**April 2021**
Review date	**October 2023**

Other Documents Policy Refers to

Document Number (if applicable)	Document Title
ICT-002	ICT Security Policy
ICT-001	ICT Acceptable Use Policy
	Data Breach Procedure
	Subject Access Request Procedure
	Guidance note – How to make a Subject Access Request
002	Staff Disciplinary Policy
	Data Protection Guidance on Police Enquiries

History of amendments

Date	Version/Pages/Sections affected	Summary of changes
April 2021	Sections 1, 5, 7, and 16	Amended text to reflect new UK GDPR legislation
April 2021	Sections 5 and 10	Amended text to reflect College's data sharing and DPIA procedures
April 2021	Section 12	Amended text to reflect College's procedures for sharing data with Police Scotland
April 2021	Sections 5 and 15	Amended text to reflect revised job titles and to correct syntax.

Contents

1 INTRODUCTION

This Policy outlines how Ayrshire College ("the College") will fulfil its obligations as a Data Controller and where applicable, a Data Processor, under current legislative provisions for data protection, data protection legislation 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 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.

4 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 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 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 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 Assistant Principal Finance, Student Funding and Estates is responsible for:

- Reporting to 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;
- Managing 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 Head of ICT 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 Estates and Sustainability 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 Assistant Principal, Human Resources (HR) and Organisational Development 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 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 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 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.

All Heads of Curriculum and Head of Services 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;
- Having a duty of care for ensuring the security of all IT systems and services within their area(s) and the protection of electronic data
- Ensuring compliance with College GDPR policies and procedures when planning and / or implementing new IT systems within their area
- 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 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 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;
- 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 six 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:

- Only collect and use personal data 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 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 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

To be able to process personal data lawfully, the College must ensure that all processing falls within one or more of the lawful bases (conditions for processing). 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 Appendix 2, 'Guide to Data Subjects Rights'.

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 Information and Customer Services Advisor 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 Information and Customer Services Advisor.

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

10 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 DPIA Screening Form 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 completed DPIA Screening Form and determine whether a full Data Protection Impact Assessment is required. For further information please contact the College's DPO by emailing dataprotection@ayrshire.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

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. A register of all Data Sharing Agreements will be maintained.

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 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 College's ICT Department).

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 one of the named officers in the 'Data Protection Guidance on Police Enquiries'. The Data Protection Officer will offer advice as required.

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.

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 a member of the Executive Leadership 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.

14 DATA RETENTION AND DISPOSAL

The College is developing and enhancing its 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, 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 is 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;
- 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 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 DPO copying in the Assistant Principal, Finance, Student Funding and Estates 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. 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 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 infringements of the 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.

17 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
- Subject Access Request Procedure
- Guidance note – How to make a Subject Access Request
- Staff Disciplinary Policy

18 LEGISLATION

18.1 Legislation relevant to this policy includes:

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

19 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.

20 DISTRIBUTION

- All Staff
- Published on College intranet
- Published on College website