Data Protection: Policy and Procedure

Policy Number	FCP2.54
Version Number	Six
Status	Approved
Approval Date: First Version	22.2.2017
Approval Date: Current Version	21.2.2024
Approved By:	Data Protection Governance Group
Responsible for Policy	Director: Governance and Compliance
Responsible for Implementation	Director: Governance and Compliance
Date of Next Review	February 2026
Equality Impact Assessed	16.04.2018
Committee Approval: Current Version	JCC – 24 June 2022

Document Change History

Document Version	Section (No. or Heading)	Description of change(s)	Date of change
6	All	• Corrected typing error • Added link to Data Sharing / Data Processor Procedure	February 2024
5	All	• Updated job titles • Updated the roles and responsibilities • Updated links	
4	All	Updated reference to UK GDPR instead of EU GDPR Updated following references: - police to Police Scotland - individual details to personal data	
3		Section 3- scope has been broadened to cover contractors Section 4 – data protection governance group added and reference to appendix 1 (also added) Section 16 – clarification re data breach framework Section 18 – link to data classification framework added	
2			
1			

Contents

1 Policy Statement

Fife College is committed to ensuring compliance with Data Protection legislation and good practice in exercising its responsibilities as a Data Controller. Fife College is registered as a Data Controller with the Information Commissioner (registration number Z8522159). The purpose of being registered as a Data Controller is to enable the College to obtain, process, disclose, retain and dispose of information about individuals (data subjects) including staff, students and graduates, in accordance with Data Protection legislation.

The two main pieces of legislation relating to Data Protection in the UK are

- UK General Data Protection Regulation (UK GDPR):
- Data Protection Act 2018 (DPA)

This policy covers Fife College and all of its wholly owned subsidiary and associated companies.

2 Purpose

The purpose of this Policy is to ensure that all staff are aware of their roles and responsibilities in relation to Data Protection and the processing of data to ensure compliance with legislation.

3 Scope

This scope of this policy extends to all members of staff and to all contractors and agencies acting for or on behalf of the College.

4 Roles and Responsibilities

The Executive Team has overall responsibility for setting the Data Protection Policy and outlining expectations of staff with regard to Data Protection.

The Director: Governance and Compliance is responsible for ensuring that the College is registered as a Data Controller with the Information Commissioner; and for ensuring that the College has appropriate arrangements in place to comply with data protection legislation.

The Data Protection Officer is responsible for providing information, training and advice to staff on Data Protection matters and for monitoring the College's compliance with legislation and policies and making recommendations for improvement and best practice. The Data Protection Officer will be the main point of contact between the College and the Information Commissioner's Office on all matters related to Data Protection.

All Directors / Heads are responsible for ensuring that all personal data being processed within their area of responsibility complies with legislation and College procedures, seeking advice where relevant from the Data Protection Team. They should ensure that staff within their Faculty / Department have completed the relevant training and have the required levels of knowledge of Data Protection and related matters in order to fulfil their roles. Where relevant, Directors / Heads are responsible for completing Privacy Impact Assessment forms and Monitoring Impact Assessment forms for activity within their areas (with support from the Data Protection Officer where required).

All members of staff are responsible for ensuring that they comply with College policies and procedures, participate in relevant training and process data in accordance with the requirements set. They should seek advice from their line manager where appropriate. All staff are expected to comply with requests from the Data Protection Team to locate personal data within given timescales where required, normally when an individual has exercised a right in relation to their personal data.

The Data Protection Governance Group acts as an ambassador for data protection matters, recommending good practice in relation to policies and procedures, and raising awareness on relevant issues. The Data Protection Governance Group has responsibility for monitoring the impact of any data breaches and making recommendations on how procedures can be improved.

Roles and Responsibilities are also highlighted in the Data Protection Governance Framework table in Appendix 1.

5 Principles Relating to Processing of Personal Data

All staff who are involved in processing data have a duty of care to ensure that such data is processed in accordance with the Data Protection Principles. Processing includes obtaining, recording, holding and storing information and carrying out any operations on the data, including adaptation, alteration, use, disclosure, transfer, erasure and destruction. Allegations of a breach with regard to this duty of care will be taken seriously and may lead to the staff disciplinary procedure being invoked.

The principles relating to processing of personal data (as outlined in the UK GDPR) are that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, not be considered to be incompatible with the initial purposes (‘purpose limitation’);
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
- 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’);
- 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);
- processed in a manner that ensures 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’)

The College must be able to demonstrate its compliance with these principles.

6 Privacy Notices

In order to be transparent, it is essential that individuals are aware of what data is being processed about them, for what purpose, and how long it will be retained for. This is outlined in Privacy Notices. Privacy Notices are made available to students as part of the application and enrolment process, and for staff as part of the job application process and at job offer stage. Privacy statements will be published on the College website and MyFife. Privacy Notice

7 Rights of the Data Subject

UK GDPR gives individuals specific rights, including:

- Right of access by the data subject (Subject Access Requests)
- Right to rectification
- Right to erasure ('Right to be Forgotten')
- Right to restriction of processing
- Right to data portability
- Right to object and automated individual decision-making (including profiling)

An information guide has been drafted on the Rights of Individuals. Information Guide

If you receive a request relating to an individual's Rights, you should pass this to the Data Protection Team as a matter of urgency, to enable it to be processed within the statutory timescale. If possible, please email the request to dpo@fife.ac.uk.

Bodies such as solicitors, local Councillors, MPs or MSPs may request information on behalf of individuals they are representing. In this case, signed consent statements from the individual must be provided before information can be considered for release.

It is important to check the identification of a person requesting information before providing it. For example, student, staff or police officer ID badges can be requested and names/numbers written on the subject access or other relevant form. Personal details should not be given out over the telephone without adequate checks being undertaken to confirm the identity of who you are speaking to.

8 Third Party Disclosures

Fife College shall only disclose personal data under one or more of the following circumstances:

- the individual has given consent
- the privacy notice specifies we will do so
- it is in the vital interests of the individual
- it is necessary for a legal obligation
- it is necessary for official authority / task carried out in the public interest
- it is a discretionary disclosure authorised by law

Police Scotland may ask the College for information when checking the safety of an individual or for the prevention and detection of crime. In these circumstances, the relevant Police Scotland form must be completed or a written request received on Police Scotland letterhead. These requests are normally straightforward and should be

processed by the relevant department as soon as possible. A Police Scotland Request for Disclosure Form must always show the names of two police officers, one of which will be of a high rank – usually a Detective Inspector. The request must state what information is required and the purpose. It must be a specific request based on evidence rather than a general wide ranging request for personal data. The College may challenge requests or ask for additional information where a request is not sufficiently focused or some information from the form is lacking. A copy of the form with a note confirming the information that was provided and date this was undertaken should be forwarded to the Director: Governance and Compliance for safekeeping. Written notification from the police is only required where personal data is requested by them about an individual (e.g. contact details, attendance record) and not where a straight forward request is being sought (e.g. a request to speak to an individual they know is currently in College; details of courses currently running).

Similarly, various agencies may contact us seeking information on students or staff, e.g. when investigating their entitlement to benefits. Provided the request is in writing, on official letterhead, and the reason for the request is clearly specified, these requests can be processed in accordance with local arrangements.

Where any request received is complex or staff are unsure of the validity of a request, advice should be sought from the relevant line manager and, where this cannot be given at a local level, by referring to the Data Protection Team.

Information may be requested by the Court in relation to legal proceedings. These requests should be passed to the Data Protection Team (email dpo@fife.ac.uk) for processing.

Where information is requested by a parent/guardian of a school age learner (i.e. learners under 16 years of age and attending a School College Partnership programme), the request should be passed immediately to the School Partnership Team. The School Partnership Team will process the request involving the relevant High School as appropriate. Where there are concerns about the safety or welfare of the learner the emergency contact held on REMs will be made aware, advice will be sought from the Department of Student Engagement and Experience and if appropriate, to Police Scotland (the relevant High School will also be notified).

Students under the age of 16 and attending full-time college (enrolled as an exceptional entrant) – the relevant manager must be aware of the under 16s enrolled on their programmes, any requests by a parent/guardian will require to be noted and actioned as appropriate. A note of the communication should be recorded (on REMS). If there are concerns about the safety or welfare of the learner the Department of Student Engagement and Experience should be contacted and/or if appropriate the police (in this situation the School Partnership Team should also be advised and they will notify the relevant High School).

Where information is requested by a parent/guardian of a learner over school age (i.e. learners over 16 years of age), these cannot be processed without the prior written consent of the learner.

9 Special Categories of Personal Data

Special categories of personal data include any information processed or that would reveal:

- racial or ethnic origin
- political opinions

- religious or philosophical beliefs
- trade-union membership
- genetic
- biometric
- health
- sex life or sexual orientation.

There are additional conditions that may be applied if any special categories of personal data are being processed. Advice from the Data Protection Officer must be sought before any such processing commences. The Data Protection Officer will escalate any residual concerns about processing to the Director: Governance and Compliance. A Data Protection Impact Assessment must also be undertaken. See also paragraph 11 below.

10 Data Protection by Design

Where any new College procedure or information system is being introduced that involves the processing of personal data, data protection implications should be considered at the earliest possible stage to ensure that all processing is in accordance with data protection principles. Advice should be sought from the Data Protection Officer as soon as practicable.

11 Data Protection Impact Assessment

Data Protection Impact Assessments are required prior to any processing taking place which is likely to result in a high risk to the rights and freedoms of individuals. In particular this should be done where processing involves new technologies or where special categories of data are being processed. It shall be the responsibility of the Director / Head to ensure Data Protection Impact Assessments are undertaken, and the advice of the Data Protection Officer should be sought. The Data Protection Officer will escalate any residual concerns to the Director: Governance and Compliance.

12 Monitoring / Profiling Activity

If the College wishes to monitor the activity of individuals or undertake any profiling activity, there must be a clear justification for this, and it must be proportionate to the College's legitimate requirements. It shall be the responsibility of the Director / Head to ensure Data Protection Impact Assessments are undertaken, advice from the Data Protection Officer should be sought before any monitoring or profiling activity commences. The Data Protection Officer will escalate any residual concerns to the Director: Governance and Compliance.

13 Complaints

If an individual is unhappy with any response given by the College, or if they are of the view that the College has breached the provisions of the Act, this can be raised with The Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF; Tel 0303 123 1113; website www.ico.org.uk.

14 Keeping Information Up-to-Date

Staff and learners must keep the College advised of any changes which may affect the data which is held in order to ensure that the data/information is current and up-to-date. There is an obligation on the College as a Data Controller to ensure that all information held is current and up-to-date, and in order to comply with this requirement, individuals may be asked from time to time to confirm that the details held about them remain accurate.

15 Secondary Access and Disclosure

Staff who have access individuals' personal data (e.g. staff, learner, clients, graduates, etc) must not use this data for personal use or to provide, reveal or disclose details to any third party, save where this is in the normal course of business. Details must not be revealed, disclosed or provided to a third party simply because the third party knows, formally or informally, that an employee does have access to or can access personal details of another.

The College will take a serious view of any data or information revealed, disclosed or provided to a third party and may invoke the staff disciplinary procedure against any member of staff suspected of doing this.

16 Data Breach Incident Management Framework

There is a requirement for the College to notify the Information Commissioner of any breaches of Data Protection which may cause harm to any individuals or organisations. All data breaches should be drawn to the attention of the Data Protection Officer as soon as they are identified, as outlined within the Data Breach Incident Management Framework. The College must notify the Information Commissioner of certain breaches within 72 hours of becoming aware of these and advise individuals affected without undue delay.

17 Advice

Advice on any aspect of Data Protection legislation or compliance should be sought in the first instance from the Data Protection Officer by emailing dpo@fife.ac.uk.

18 Other Relevant Documents

CCTV Policy
Data Breach Incident Management Framework
Data Classification and Data Handling Framework
Data Protection - Your Rights
Data Protection Impact Assessment Form
Data Sharing / Data Processor Procedure
Digital Acceptable Use Policy
Document Retention Policy and Procedure
Information Security Policy
Privacy Notice
Subject Access Request Form

Key

Accountable	A	person who performs an activity or does the work.
Responsible	R	person who is ultimately accountable and has Yes/No/Veto
Consulted	C	person that needs to feedback and contribute to the activity
Informed	I	person that needs to know of the decision or action

	Executive Team	Director: Governance and Compliance	Data Protection Officer	Governance and Delivery Manager	Data Protection Governance Group	Directors / Heads	Staff
Setting Data Protection Policy	A	R	R	C	C	I	I
Appointing Data Protection Officer	A	R	I	I	I	I	I
Data Controller Registration	R	A	R	I	I	I	I
Ensuring lawful processing within area of responsibility	I	C	C	C	I	A	R
Completing Privacy Impact Assessment forms	I	C	C	C	C	A	R
Reporting Data Breaches to DPO/DGM	I	I	R	R	C	A	R
Reporting Data Breaches to Information Commissioner	I	A	R	C	R	I	I
Recommending changes to processes as a result of breaches of audits	I	A	A	A	R	R	I
Undertaking data protection audits	R	R	A	C	I	C	I
Recommending actions as a result of findings of data protection audits	I	A	A	A	R	I	I
Ensuring appropriate training is provided to staff	A	R	R	I	C	R	I
Ensuring staff participate in training	A	I	I	I	I	A	R
Ensuring Data Sharing Agreements are in place	R	A	A	I	C	R	I