Policy Title — Data Protection/Data Management

Author/Responsible Manager	Director of Governance
Original Issue Date	May 2009
Approved By and Date	February 2020 Audit & Risk Committee
Next Review Date	February 2022
EIA Completion date	
Risk Assessment (please note here any identified risks of non-compliance with the policy)	Breach of Data Protection Act 1998 Breach of Freedom Of Information Act 2000 Breach of GDPR Regulations

CONTENTS **PAGE NUMBER**

Equality Impact Assessment **1**

Introduction **2**

Policy Statement **2**

Procedure **2**

Reference to Other Policies **14**

Equality Impact Assessment				
Characteristic	No impact	Positive impact	Negative impact	Evidence
Race	☒	☐	☐	
Disability	☒	☐	☐	
Gender	☒	☐	☐	
Pregnancy/Maternity	☒	☐	☐	
Religion/belief	☒	☐	☐	
Sexual orientation	☒	☐	☐	
Age	☒	☐	☐	
Gender reassignment	☒	☐	☐	
Marriage & civil partnership	☒	☐	☐	
Carried out by: C Drury				

Actions required:

Action	Date	Reviewed by	Date

1 Introduction

Kendal College needs to keep certain information about its employees, students and other users to allow it to receive funding, monitor its performance, achievements and operate effectively. It is also necessary to process information so that staff can be recruited and paid, so that courses can be organised and various legal obligations to funding bodies and government complied with.

To comply with legislation, information must be collected and used fairly, stored securely and not disclosed to any person unlawfully. To do this, the College must comply with the principles set out in the General Data Protection Regulation (GDPR) as it applies in the UK, tailored by the Data Protection Act 2018. The College is also committed to meeting its legal requirements under the Freedom of Information Act 2000 and the GDPR that places greater emphasis on demonstration of accountability of data management.

This policy should be read in conjunction with the Freedom of Information Policy and the Document Retention policy along with other policies linked to GDPR listed at the end of this policy. The policy also applies to provision delivered in partnership with other providers and for all students/ learners who receive training in the College's name.

2 Policy Statement

The College will ensure that all personal data is processed fairly and lawfully, including under the requirements of GDPR.

Any member of staff who considers that this policy has not been followed in respect of personal data about themselves or other college users, should raise the matter with the appointed Data Protection Officer initially. The College has a nominated Data Protection Controller; the Director of Governance (see below)

In all instances, a legal basis for holding personal information is established and recorded by the College. The following lawful purposes for processing ordinary Personal Data as set out in Article 6 of the GDPR and are as follows (paraphrased):

- the use of the Personal Data for the purposes of the legitimate interests of the Controller ie the College;
- the processing is necessary for the performance of a contract ~~(eg ESFA, HEFCE~~);
- the processing is necessary for compliance with a legal obligation;
- the processing is necessary in order to protect the vital interests of the individual or of another natural person (eg health & safety or safeguarding);
- the processing is necessary for the performance of a task carried out in the public interest; and
- the individual who is the subject of the Personal Data has given consent for one or more specific purposes (eg restaurant, salon bookings).

Most data held by the college uses the legal basis of public task or legitimate interest and relies on consent only as a last resort.

This policy should be read in conjunction with four key additional policies:

a. Rights of Individuals including Subject Access Requests
b. Personal Data Breach Notification
c. Information Sharing
d. Records Management & Data Retention schedule

3 Key Definitions

Controller – Any entity (e.g. company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data ie the College.

The College has registered under the Act with the Information Commissioner using the template provided for FE establishments. The College has a designated Data Protection Controller (Director of Governance), who is responsible for the College registration under the Act and for compliance with GDPR.

Data Protection Laws – The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Acts of 1998 and 2018

Data Protection Officer – Our Data Protection Officer is:
Director of Governance, ~~Carole Drury carole.drury@kendal.ac.uk or~~ who can be contacted via the following email address: dataprotection@kendal.ac.uk ~~In her absence, reference should be made to Assistant Principal, Corporate Resources – Louise Shrapnel (01539 814705)~~ the email address is also monitored by a designated member of the senior leadership team to provide continuity of service.

Personal Data – Any information about an Individual which identifies them or allows them to be identified in conjunction with other information that is held. It includes information of this type, even if used in a business context.

Personal data is defined broadly and covers things such as name, address, email address (including in a business context, email addresses of Individuals in companies such as firstname.surname@organisation.com), IP address and also more sensitive types of data such as trade union membership, genetic data and religious beliefs.

Processor – Any entity (eg company, organisation or person) which accesses or uses Personal Data on the instruction of a Controller. A Processor is a third party that processes Personal Data on behalf of a Controller. This is usually as a result of the outsourcing of a service by the Controller or the provision of services by the Processor which involve access to or use of Personal Data. Examples include: where software support for a system, which contains Personal Data, is provided by someone outside the business; cloud arrangements; and mail fulfilment services. Wherever personal data is processed on the authority of the controller, a data sharing agreement is put in place to provide assurance on the security of the data.

Special Categories of Personal Data – Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (ie information about their inherited or acquired genetic characteristics), biometric data (ie information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

4 General Data Protection Regulation Principles

4.1 When using Personal Data, Data Protection Laws require that the College complies with the following principles. These principles require Personal Data to be:

a. processed lawfully, fairly and in a transparent manner;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
c. adequate, relevant and limited to what is necessary for the purposes for which it is being processed;

d. accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible;

e. kept for no longer than is necessary for the purposes for which it is being processed; and
f. 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.

These principles are considered in more detail in the remainder of this Policy. In addition to complying with the above requirements, the College also has to demonstrate in writing that it complies with them. The College has a number of policies and procedures in place, including this Policy and the documentation referred to in it, to ensure that the College can demonstrate its compliance.

The following actions are in place to ensure the College meets its statutory obligations under the Regulation:

a. Awareness raising for key managers, governors and staff within the College on understanding the impact of the legislation and compliance requirements, including through training

b. Documenting personal information that is held by the College including its source and where it is shared through an information audit, noting the legal basis for collection and processing to form the basis of an information asset register. Legal basis can be checked using this link - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing

c. Where special category data is collected, the College has to show that one of a number of additional conditions is met. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/special-category-data

d. Providing comprehensive and clear information to staff, students and other stakeholders about how we will use their information and how long it will be retained via privacy notices

e. Reviewing College processes for deleting personal data and electronic records including direct marketing implications

f. Reviewing how the College responds to subject access requests within new reduced time limits (see separate policy)

g. Reviewing where consent is required and recorded with an effective audit trail, including parental or guardian consent

h. Reviewing procedures for detecting, reporting and investigating personal data breach (see separate policy)

i. Implementing a process to carry out Privacy Impact Assessments in high risk situations

j. Annual reviewing of the policy and annual reporting to the Corporation on compliance and impact

5 Responsibilities of Staff

All College employees must comply with this policy and ensure they never release or disclose personal information to staff who are not authorised to access personal data. It is also staff responsibility to see that the College only collects and processes Personal Data to the extent that it is required for the specific purpose(s) notified to the individual in a privacy notice and as set out in the College's record of how it uses Personal Data.

All College employees must ensure that they keep confidential all Personal Data that they collect, store, use and come into contact with during the performance of their duties

All staff, including those of other organisations delivering on behalf of the College, are responsible for:

- checking that their own personal information provided to the College in connection with their employment is accurate and up to date
- informing the College of any errors or changes to information, ie change of address

If, and when, as part of their responsibilities, staff collect information on others (ie students, references, details of personal circumstances), they must comply with all procedure on the management of personal data. This includes the following key practices:

a. Adopting the concept of "tidy desk" whereby there is no risk of student personal data being inadvertently shared.
b. Locking away all student data when not at your desk
c. Never leaving your desktop or laptop open when away from your desk
d. Not leaving unattended student data or files in cars or other locations away from the college
e. Ensuring that no data is transferred outside the College without appropriate security measures being applied such as data encryption and two-factor authentication
f. Checking if a data sharing agreement is in place when data needs to be shared with another processing organisation
g. Attend training as part of staff development programme

The Data Protection Officer is responsible for:

a. Keeping this policy updated and relevant
b. Ensuring that the College complies with the Data Protection Acts 1998/2018 including the General Data Protection Regulation
c. Producing an annual report to the Board on compliance with GDPR and instances of breach
d. Ensuring that relevant and appropriate training is held including induction of new staff

6 Privacy Notices

The College must be transparent with individuals about how their Personal Data will be used. This is generally done through a privacy notice. All privacy notices developed for different types of users must display:

a. the identity and the contact details of the Controller (ie the College)
b. the contact details of the Data Protection Officer, where applicable;

c. the purposes the Personal Data will be used for as well as the legal basis for the processing;
d. if legitimate interests is used as a lawful purpose, the legitimate interest must be specified;
e. the recipients/categories of recipients of the Personal Data, if any;
f. details of data export and the safeguards applied;
g. the period the Personal Data will be stored;
h. the right to request access to, rectification or erasure of Personal Data;
i. the right to request restriction of use of the Personal Data, the right to object to use as well as the right to data portability;
j. where the individual has given consent, the right to withdraw that consent;
k. the right to lodge a complaint with the ICO;
l. the existence of automated decision making including profiling, the logic involved, as well as the significance and envisaged consequences;
m. whether the provision of the data is a statutory or contractual obligation and of the possible consequences of failure to provide such data; and
n. if the Controller intends to further process the Personal Data, provide the individual with information on such further processing.

Where the College collects Personal Data directly from Individuals, the College will inform them about how the College uses their Personal Data. This is in a privacy notice. Examples of privacy notices currently in use by the College include:

- General college Privacy Notice – College website
- Full time course application form
- Course enrolment forms

If the College receives Personal Data about an Individual from other sources, the College will provide the Individual with a privacy notice about how the College will use their Personal Data to be provided as soon as reasonably possible and in any event within one month.

If the College changes how it uses Personal Data, the College may need to notify Individuals about the change. If staff therefore intend to change how they use Personal Data please notify the Data Protection Officer who will decide whether the intended use requires amendments to be made to the privacy notices and any other controls which need to apply.

7 Appointing Contractors Who Access The College's Personal Data

If the College appoints a contractor who is a Processor of the College's Personal Data, Data Protection Laws require that the College only appoints them where the College has carried out sufficient due diligence and only where the College has appropriate contracts in place.

One requirement of GDPR is that a Controller must only use Processors who meet the requirements of the GDPR and protect the rights of individuals. This means that data protection due diligence should be undertaken on both new and existing suppliers. Once

a Processor is appointed they should be audited periodically to ensure that they are meeting the requirements of their contract in relation to Data Protection.

Any contract where an organisation appoints a Processor must be in writing.

You are considered as having appointed a Processor where you engage someone to perform a service for you and as part of it they may get access to your Personal Data. Where you appoint a Processor you, as Controller remain responsible for what happens to the Personal Data.

GDPR requires the contract with a Processor to contain the following obligations as a minimum:

a. to only act on the written instructions of the Controller through the signing of a Data Sharing agreement;

b. to not export Personal Data without the Controller's instruction;

c. to ensure staff are subject to confidentiality obligations;

d. to take appropriate security measures;

e. to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;

f. to keep the Personal Data secure and assist the Controller to do so;

g. to assist with the notification of Data Breaches and Data Protection Impact Assessments;

h. to assist with subject access/individuals rights;

i. to delete/return all Personal Data as requested at the end of the contract;

j. to submit to audits and provide information about the processing; and

k. to tell the Controller if any instruction is in breach of the GDPR or other EU or member state data protection law.

In addition the contract should set out:

a. The subject-matter and duration of the processing;

b. the nature and purpose of the processing;

c. the type of Personal Data and categories of individuals; and the obligations and rights of the Controller

8 Marketing and Consent

The College will sometimes contact Individuals to send them marketing materials or to promote the College. Where the College carries out any marketing, Data Protection Laws require that this is only done in a legally compliant manner. Marketing consists of any advertising or marketing communication that is directed to particular individuals. GDPR requires a number of important changes for organisations that market to individuals, including:

- Providing more detail in their privacy notices, including for example whether profiling takes place

- Rules on obtaining consent are stricter and will require an individual's "clear affirmative action"

The College is required to comply with the Privacy and Electronic Communications Regulations (PECR) that sit alongside data protection and applies to direct marketing ie a communication directed to particular individuals and covers any advertising/marketing material. It applies to electronic communication ie calls, emails, texts, faxes. PECR rules apply even if personal data is not being processed.

Consent is central to electronic marketing. Best practice is to provide an un-ticked opt-in box.

Alternatively, the College is permitted to market using a “soft opt in” if the following conditions were met:

a. contact details have been obtained in the course of a sale (or negotiations for a sale);
b. the College is marketing its own similar services; and
c. the College gives the individual a simple opportunity to opt out of the marketing, both when first collecting the details and in every message after that.

9 Data Protection Impact Assessments (DPIA)

The GDPR introduced a new requirement to carry out a risk assessment in relation to the use of Personal Data for a new service, product or process. This must be done prior to the processing via a Data Protection Impact Assessment (“DPIA”). A DPIA should be started as early as practical in the design of processing operations. A DPIA is not a prohibition on using Personal Data but is an assessment of issues affecting Personal Data which need to be considered before a new product/service/process is rolled out. The process is designed to:

a. describe the collection and use of Personal Data;

b. assess its necessity and its proportionality in relation to the purposes;

c. assess the risks to the rights and freedoms of individuals; and

d. the measures to address the risks.

A DPIA must be completed where the use of Personal Data is likely to result in a high risk to the rights and freedoms of individuals. A DPIA template is available at appendix 1. Where a DPIA reveals risks which are not appropriately mitigated, the ICO must be consulted.

Where the College is launching or proposing to adopt a new process, product or service which involves Personal Data, the College needs to consider whether it needs to carry out a DPIA as part of the project initiation process. The College needs to carry out a DPIA at an early stage in the process so that the College can identify and fix problems with its proposed new process, product or service at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

Situations where the College may have to carry out a Data Protection Impact Assessment include the following (please note that this list is not exhaustive):

- large scale and systematic use of Personal Data for the purposes of Automated Decision Making or Profiling where legal or similarly significant decisions are made;

- large scale use of Special Categories of Personal Data, or Personal Data relating to criminal convictions and offences e.g. the use of high volumes of health data; or

- systematic monitoring of public areas on a large scale e.g. CCTV cameras.

All DPIAs must be reviewed and approved by the Data Protection Officer.

11 Conclusion

Compliance with the Data Protection Act 2018 and the introduction of the General Data Protection Regulation is the responsibility of all members of the College and associated delivery staff, and staff should be mindful of the following:

- No undue pressure should be placed on anyone to disclose personal data
- No personal data should be disclosed over the telephone unless the caller has been properly identified and is entitled to the data
- Any special request for disclosure of personal data, eg to the Police or Inland Revenue, should be referred to the Data Protection Officer who will manage and log the request
- Personal data must be disposed of in a way that protects the rights and privacy of data subjects (eg shredding, disposal as confidential waste, secure electronic deletion).

12 Linked policies

- Freedom of Information Policy
- Document Retention Policy
- IT User Policy
- Information sharing
- Data retention – which details how long you hold personal data for;
- Policies that implement individuals rights, including subject access requests; and
- Data breach reporting.