Document Title: **Data Protection Policy**

Document Ref: **HE/006**

Approved By: **Chris Nattress**

Author: Karen Wilson

Responsible Board: **Higher Education Academic Board**

Date last reviewed: **23/11/2023**

Date of next review: **22/11/2024**

Approval date: **23/11/2023**

Document Change Log	
Summary of changes made between previous issue and this current issue	Page number

If you require this document in an alternative format (such as large print, Braille, printed on coloured paper or a paper copy of an electronic document), please use the following email address:

- info@lcwc.ac.uk

Contents

1 Summary of this document 3
2 Scope 3
3 Responsibility 3
4 Introduction 5
Data Protection Policy 5
5 Data Protection Personnel's General Obligations 5
5.1 Definitions 6
5.2 Data Protection Principles 8
5.3 Lawful use of personal data 9
5.4 Transparent Processing – Privacy Notices 9
5.4 Data Quality – Ensuring the use of accurate, up-to-date and relevant personal data 10
5.5 Personal Data Retention 11
5.6 Data Security 12
5.7 Data Breach 12
5.7.1 Containment of Data Breach 14
5.7.2 Assessment of ongoing risk 14
5.7.3 Notification 14
5.7.4 Evaluation and Response 16
5.8 Appointing Contractors 16
5.9 Individual's rights (Data Subject) 18
5.9.1 **Subject Access Requests** 19
5.9.2 **Right of Erasure (Right to be Forgotten)** 19
5.9.3 **Right of Data Portability** 20
5.9.4 **The Right of Rectification and Restriction** 20
5.10 Marketing and consent 20
5.11 Automated decision making and profiling 21
5.12 Data Protection Impact Assessment (DPIA) 22
5.13 Transferring personal data to a country outside the EEA 24
6 Complaints 25
7 Other relevant policies and procedures 25
8 Any external references 25

1 Summary of this document

The Institution's reputation and growth are dependent on the way we manage and protects Personal Data Protecting the confidentiality and integrity of Personal Data is a key responsibility of everyone within the institution.

We are an organisation which collects, uses and stores personal data about its employees, suppliers, enquirers, applicants, students (current and former), governors, parents, visitors and wider stakeholders. We recognise that having controls around the collection, use, retention and destruction of Personal Data is important in order to comply with our legal obligations under Data Protection Act (2018) and in particular under Article 5 of GDPR

2 Scope

Our Higher Education Data Protection Policy applies to, and must be adhered to, by all staff processing personal data for the Institution. The term all staff for this policy includes:

- Senior managers and directors;
- Employees (this includes permanent, fixed-term, temporary, or casual);
- Agency, contract, and seconded staff;
- Volunteers, apprentices, and interns; and
- Other associated with the Institution e.g consultants.

You should be aware of your rights as a student as a data subject and the Institution's responsibilities with regards to your own personal data.

Third parties who process personal data for the Institution have obligations under Data Protection legislation that those engaging them must be aware.

This policy will also apply to students who are also staff of the Institution who process personal data as part of their role.

3 Responsibility

Title	Responsibility

Board of Governors	It is a collective responsibility of the Board of Governors to ensure that the legislative duties placed on the College are met.
The Dean of HE	Has overall responsibility for the strategic management of Higher Education Assessment Policy, monitoring of achievements and for the implementation of plans for improvements in outcomes for learners.
All staff	Are responsible for familiarising themselves with this policy and must ensure that they adhere to the data protection principles when processing personal data as part of their work for the Institution Are required to complete data protection training as required.
The Data Protection Officer	Is responsible for monitoring internal compliance with data protection legislation, informing and advising on data protection obligations, providing advice in relation to Data Protection Impact Assessments, and acting as a contact point for data subjects and the Information Commissioner's Office (ICO)

If you have any questions in relation to the HE Data Protection Policy, please contact info@lcwc.ac.uk

Data Officer Details:

Name: Karen Wilson Email: karenw@lcwc.ac.uk

Phone: 01946839300

ICO Registration: Z8613891 Information Commissioner's Office - Register of data protection fee payers - Entry details (ico.org.uk)

4 Introduction

The HE Data Protection Policy is to ensure all Institution Personnel are aware of what they must do to ensure the correct and lawful treatment of Personal Data.

All Personnel will receive a copy of this policy during their induction and may receive periodic revisions of this Policy. This Policy does not form part of any member of the Personnel's contract of employment and we reserve the right to change this Policy subject to legal and regulatory requirements.

Data Protection Policy

5 Data Protection Personnel's General Obligations

All Institution Personnel must comply with this policy.

Institution Personnel 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.

Institution Personnel must not release or disclose any Personal Data:

- outside the Institution; or
- inside the Institution to Institution Personnel not authorised to access the Personal Data,
- without specific authorisation from their manager or the Data Protection Officer; this includes by phone calls or in emails.
- Institution Personnel must take all steps to ensure there is no unauthorised access to Personal Data whether by other Institution Personnel who are not authorised to see such Personal Data or by people outside the Institution.
- Institution Personnel are advised that any breach of this Data Protection Policy will be treated seriously and may result in disciplinary action.

5.1 Definitions

Note: This paragraph 3 includes definitions of the most relevant data protection terms. The definitions are based on the definitions contained in the GDPR, but include additional plain English explanations of the various terms.

1) **Institution** – Lakes College West Cumbria
2) **Institution Personnel** – Any Institution employee, worker or contractor who accesses any of the Institution's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the Institution.
3) **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.

   A Controller is responsible for compliance with Data Protection Laws. Examples of Personal Data the Institution is the Controller of include employee details or information the Institution collects relating to students. The Institution will be viewed as a Controller of Personal Data if it decides what Personal Data the Institution is going to collect and how it will use it.

   A common misconception is that individuals within organisations are the Controllers. This is not the case it is the organisation itself which is the Controller.
4) **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 Act 2018.

5) **Data Protection Officer –** Our Data Protection Officer is Karen Wilson, and can be contacted at 01946 839300 ext. 1010, karew@lcwc.ac.uk

6) **EEA** – Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.
7) **ICO** – the Information Commissioner's Office, the UK's data protection regulator.
8) **Individuals** – Living individuals who can be identified, *directly or indirectly*, from information that the Institution has. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location if you can use this information to work out who they are. Individuals include employees, students, parents, visitors and potential students. Individuals also include partnerships and sole traders.
9) **Personal Data** – Any information about an Individual (see definition above) 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. These more sensitive types of data are called "Special Categories of Personal Data" and are defined below. Special Categories of Personal Data are given extra protection by Data Protection Laws.
10) **Processor** – Any entity (e.g. 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.

11) **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 (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. 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. Criminal offence data is subject to additional protection as is special category data and it is officially a separate category of data. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

5.2 Data Protection Principles

Data protection legislation outlines the following principles that must be adhered to when processing personal data:

- Processed lawfully, fairly and in a transparent manner;

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary for the purposes for which it is being processed;
- 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;
- kept for no longer than is necessary for the purposes for which it is being processed; and

- 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.

The data controller is responsible for and must be able to demonstrate compliance with the above.

5.3 Lawful use of personal data

5.3.1 In order to collect and/or use Personal Data lawfully the Institution needs to be able to show that its use meets one of a number of legal grounds. Please click here to see the detailed grounds: [https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing]

5.3.2 In addition, when the Institution collects and/or uses Special Categories of Personal Data, the College has to show that one of a number of additional conditions is met. Please click here to see the detailed additional conditions [Special category data | ICO. Further information on the College's processing of special category data and criminal offences data can be found in the College's Appropriate Policy Document which supplements the College's privacy notices.

5.3.3 The Institution has carefully assessed how it uses Personal Data and how it complies with the obligations set out in paragraphs 5.3.1 and 5.3.2. If the Institution changes how it uses Personal Data, the Institution needs to update this record and may also need to notify Individuals about the change. If the Institution's Personnel therefore intend to change how they use Personal Data at any point they must notify the Data Protection Officer who will decide whether their intended use requires amendments to be made and any other controls which need to apply.

5.4 Transparent Processing – Privacy Notices

Where the Institution collects Personal Data directly from Individuals, the Institution will inform you about how we will use your Personal Data. This is in a privacy notice. Personal data will be processed and shared within the boundaries of principals of data protection. Data will be retained as set out in the HE Data Retention Policy.The College has adopted the following privacy notices: applicants, students, former students, college

personnel, governors, stakeholders and partners, suppliers, customer, web-site users.

a. If the Institution receives Personal Data about a data subject (you) from other sources, the Institution will provide you with a privacy notice about how the Institution will use your Personal Data. You will be informed where the personal data was obtained from. This will be provided as soon as reasonably possible and in any event within one month.

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

5.4 Data Quality – Ensuring the use of accurate, up-to-date and relevant personal data

a. Data Protection legislation require the Institution 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 (see paragraph 5.4 above) and as set out in the Institution's record of how it uses Personal Data. The Institution is also required to ensure that the Personal Data the Institution holds is accurate and kept up to date.

b. All Personnel that collect and record Personal Data shall ensure that the Personal Data is recorded accurately, is kept up to date and shall also ensure that they limit the collection and recording of Personal Data to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used.

c. All Personnel that obtain Personal Data from sources outside the Institution shall take reasonable steps to ensure that the Personal Data is recorded accurately, is up to date and limited to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. If information has been provided to the Institution, we will take reasonable steps to ensure that the data is accurate, having regard to the importance of the information and the potential consequences of inaccuracy, or if common sense suggests that there may be a mistake.

d. In order to maintain the quality of Personal Data, all Institution Personnel that access Personal Data shall ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. Please note that this does not apply to Personal Data which the Institution must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

e. The Institution recognises the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws. The Institution has a Rights of Individuals Policy and a Rights of Individuals Procedure which set out how the Institution responds to requests relating to these issues. Any request from an individual for the amendment, rectification, erasure or restriction of the use of their Personal Data should be dealt with in accordance with those documents.

5.5 Personal Data Retention

- Data Protection Laws require that the Institution does not keep Personal Data longer than is necessary for the purpose or purposes for which the Institution collected it.

- The Institution has assessed the types of Personal Data that it holds and the purposes it uses it for and has set retention periods for the different types of Personal Data processed by the Institution, the reasons for those retention periods and how the Institution securely deletes Personal Data at the end of those periods. These are set out in the Data Retention Policy.

- If Institution Personnel feel that a particular item of Personal Data needs to be kept for more or less time than the retention period set out in the Data Retention Policy, for example because there is a requirement of law, or if Institution Personnel have any questions about this Policy or the Institution's Personal Data retention practices, they should contact the Data Protection Officer for guidance.

5.6 Data Security

The Institution takes information security very seriously and we have security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. We have in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

5.7 Data Breach

a. We take information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of Personal Data. If this happens there will be a Personal Data breach and our Personnel must comply with the Institution's Data Breach Notification Policy. Please see paragraphs 11C for examples of what can be a Personal Data breach. Please familiarise yourself with it as it contains important obligations which our Personnel need to comply with in the event of Personal Data breaches.

b. Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of Personal Data. Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal does.

c. There are three main types of Personal Data breach which are as follows:

i. **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that a College Personnel is not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people "blagging" access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information over the phone to the wrong person;

ii. **Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from back up, or loss of an encryption key; and

iii. **Integrity breach** - where there is an unauthorised or accidental alteration of Personal Data.

5.7.1 Containment of Data Breach

An initial assessment of the impact of the Personal Data breach will be carried out by the Data Protection Officer in consultation with appropriately qualified staff in relation the nature of the breach.

If the Personal Data breach is unlikely to result in a risk to the rights and freedoms of the individuals **affected,** then it will be added to the **Institution**'s Data Breach Register and no further action will be taken.

If the Personal Data breach may impact on the rights and freedoms of the individual affected, then the **Institution** will put together and implement a bespoke Personal Data breach plan to address the breach concerned in accordance with the **Institution**'s Data Breach Notification Procedure.

All actions taken in relation to a Personal Data breach will be in accordance with the Data Breach Notification Procedure which is maintained and administered by the Data Protection Officer.

The Data Protection Officer is responsible for ensuring that the Data Breach Register is updated.

5.7.2 Assessment of ongoing risk

As part of our response to a Personal Data breach, once the breach has been contained we will consider the on-going risks to the Institution and to any other party caused by the breach and what remedial action can be taken to minimise the impact of the breach. This will be undertaken in accordance with the Institution's Data Breach Notification Procedure.

5.7.3 Notification

Under Data Protection Laws, we may have to notify the ICO and also possibly the individuals affected about the Personal Data breach.

Any notification will be made by the Data Protection Officer following the College's Data Breach Notification Procedure. The notification shall comply with the requirements of the ICO.

Notification of a Personal Data breach must be made to the ICO without undue delay and where feasible within **72 hours of** when we become aware of the breach unless it is *unlikely to result in a risk to the rights and freedoms of individuals*. It is therefore imperative that the Institution's Personnel notify all Personal Data breaches to the Data Protection Officer or Executive Support in accordance with the Data Breach Notification Procedure immediately.

Notification of a Personal Data breach must be made to the individuals affected without undue delay where the breach is *likely to result in a high risk to the rights and freedoms of individuals.*

Please note that not all Personal Data breaches are notifiable to the ICO and/or the individuals affected and the College will decide whether to notify and who to notify in accordance with the Data Breach Notification Procedure.

Where the Personal Data breach relates to a temporary loss of availability of the Institution's systems, the Institution does not have to notify if the lack of availability of Personal Data is unlikely to result in a risk to the rights and freedoms of individuals. The Institution does not consider that it has any systems where temporary unavailability would cause a risk to the rights and freedoms of individuals but this will be assessed on a case-by-case basis in accordance with the Data Breach Notification Procedure.

In the case of complex breaches, we may need to carry out in-depth investigations. In these circumstances, we will notify the ICO with the information that it has within 72 hours of awareness and will notify additional information in phases. Any delay in notifying the ICO must be seen as exceptional and shall be authorised in accordance with the Data Breach Notification Procedure.

Where a Personal Data breach has been notified to the ICO, any changes in circumstances or any relevant additional information which is discovered in

relation to the Personal Data breach shall also be notified to the ICO in accordance with the Data Breach Notification Procedure.

When the Institution notifies the affected individuals, it will do so in clear and plain language and in a transparent way. Any notifications to individuals affected will be done in accordance with the Data Breach Notification Procedure. Any notification to an individual should include details of the action the Institution has taken in relation to containing the breach and protecting the individual. It should also give any advice about what they can do to protect themselves from adverse consequences arising from the breach.

We may not be required to notify the affected individuals in certain circumstances as exemptions apply. Any decision whether to notify the individuals shall be done in accordance with the Data Breach Notification Procedure and shall be made by the Data Protection Officer.

5.7.4 Evaluation and Response

It is important not only to investigate the causes of the breach but to document the breach and evaluate the effectiveness of our response to it and the remedial action taken.

There will be an evaluation after any breach of the causes of the breach and the effectiveness of our response to it. All such investigations shall be carried out in accordance with the Data Breach Notification Procedure and will be recorded on the Personal Data Breach Register.

Any remedial action such as changes to our systems, policies or procedures will be implemented in accordance with the Data Breach Notification Procedure.

5.8 Appointing Contractors

a. If we appoint a contractor who is a Processor of the Institution's Personal Data, Data Protection Laws require that the Institution only appoints them where we have carried out sufficient due

diligence and only where we have the appropriate contracts in place.

b. One requirement of GDPR is that a Controller must provide guarantees to implement appropriate measures to ensure the processing of data complies with the UK GDPR and protect the rights of individuals.

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

d. An appointment of a Processor can include the engagement of someone to perform a service for you and as part of it they may get access to your Personal Data. Where an appointment of a Processor, the Data Controller remains responsible for what happens to the Personal Data and for the compliance with the relevant legislation

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

i. to only act on the written instructions of the Controller;

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

iii. to ensure staff are subject to confidentiality obligations;

iv. to take appropriate security measures;

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

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

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

viii. to assist with subject access/individuals rights;

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

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

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

f. In addition the contract should set out:

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

ii. the nature and purpose of the processing;

iii. the type of Personal Data and categories of individuals; and

iv. the obligations and rights of the Controller.

5.9 Individual's rights (Data Subject)

GDPR gives individuals more control about how their data is collected and stored and what is done with it. Some existing rights of individuals have been expanded upon and some new rights have been introduced.
We will use all Personal Data in accordance with the rights given to Individuals' under Data Protection Laws, and will ensure that it allows

Individuals to exercise their rights in accordance with the Institution's Rights of Individuals Policy and Rights of Individuals Procedure. Please familiarise yourself with these documents as they contain important obligations which our Personnel need to comply with in relation to the rights of Individuals over their Personal Data.

The different types of rights of individuals are reflected in this paragraph.

5.9.1 **Subject Access Requests**

Individuals have the right under the GDPR to ask the Institution to confirm what Personal Data they hold in relation to them and provide them with the data.

Subject Access Requests are becoming more and more common and are often made in the context of a dispute which means that it is crucial that they are handled appropriately to avoid a complaint being made to the ICO.

Any learner subject access request will be notified to the Education Skills Funding Agency (ESFA) within 5 working days as per the Financial Memorandum (Further Education Colleges).

5.9.2 **Right of Erasure (Right to be Forgotten)**

This is a limited right for individuals to request the erasure of Personal Data concerning them where:

1. the use of the Personal Data is no longer necessary;
2. their consent is withdrawn and there is no other legal ground for the processing;
3. the individual objects to the processing and there are no overriding legitimate grounds for the processing;
4. the Personal Data has been unlawfully processed; or

5. the Personal Data has to be erased for compliance with a legal obligation.

In a marketing context, where Personal Data is collected and processed for direct marketing purposes, the individual has a right to object to processing at any time. Where the individual objects, the Personal Data must not be processed for such purposes.

5.9.3 **Right of Data Portability**

An individual has the right to request that data concerning them is provided to them in a structured, commonly used and machine readable format where:

1. the processing is based on consent or on a contract; and
2. the processing is carried out by automated means

Alternatively, you as an individual have the right to request that the data controller transmit your personal data directly to another controlled.
This right isn't the same as subject access and is intended to give individuals a subset of their data.

5.9.4 **The Right of Rectification and Restriction**

Finally, individuals are also given the right to request that any Personal Data is rectified if inaccurate and to have use of their Personal Data restricted to particular purposes in certain circumstances.

5.10 Marketing and consent

We will sometimes contact individuals to send them marketing materials or to promote the Institution. Where we carry out any marketing, Data Protection Laws require that this is only done in a legally compliant manner.

Direct marketing consists of any advertising or marketing communication that is directed to particular individuals. GDPR emphasises the key requirements of an organisations that market to individuals, including:

1. providing more detail in privacy notices, including for example whether profiling takes place; and
2. rules on obtaining consent around direct marketing material

The Privacy and Electronic Communications Regulations (PECR) that sit alongside data protection and gives you specific privacy rights in relation to electronic communications. PECR apply to direct marketing i.e. a communication directed to particular individuals and covers any advertising/marketing material. It applies to electronic communication i.e. calls, emails, texts, faxes. PECR rules apply even if you are not processing any personal data and applies to unsolicited direct marketing.

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

We may be able to market using a “soft opt in” if the following conditions are met:

1. contact details have been obtained in the course of a sale (or negotiations for a sale);

2. we are marketing its own similar services; and

We give the individual a simple opportunity to opt out of the marketing, both when first collecting the details and in every message after that.

5.11 Automated decision making and profiling

Under Data Protection Laws there are controls around profiling and automated decision making in relation to Individuals.

Automated Decision Making is a decision made by automated means without any human involvement.

Profiling is the automated processing of personal data to evaluate certain things about an individual.

Any Automated Decision Making or Profiling which we carry out can only be done once we are confident that it is complying with Data Protection Laws.

Institution Personnel must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.

We do not carry out Automated Decision Making or Profiling in relation to its employees.

5.12 Data Protection Impact Assessment (DPIA)

Under data protection legislation, we are required to complete a Data Protection Impact Assessment (DPIA) for types of processing that are likely to result in high risk to the rights and freedoms of data subjects.

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:

- describe the collection and use of Personal Data;
- assess its necessity and its proportionality in relation to the purposes;
- assess the risks to the rights and freedoms of individuals; and
- 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. The ICO's standard DPIA template is available from www.ico.org.uk.

Where a DPIA reveals risks which are not appropriately mitigated the ICO must be consulted.

Where we are launching or proposing to adopt a new process, product or service which involves Personal Data, we will need to consider whether it needs to carry out a DPIA as part of the project initiation process. The Institution's needs to carry out a DPIA at an early stage in the process so that we 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.

There are certain circumstances in which the GDPR requires a DPIA to be completed i.e. if you plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

The ICO also requires completion of a DPIA if you plan to:

- use innovative technology (in combination with any of the criteria from the European guidelines);
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data (in combination with any of the criteria from the European guidelines);
- process genetic data (in combination with any of the criteria from the European guidelines);
- match data or combine datasets from different sources;

- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing') (in combination with any of the criteria from the European guidelines);
- track individuals' location or behaviour (in combination with any of the criteria from the European guidelines);
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

Outside of these circumstances in which is DPIA is mandatory, the trigger for completion of a DPIA is where the use of personal data is likely to result in a high risk to the rights and freedoms of individuals.

All DPIAs must be reviewed and approved by the Data Protection Officer. Please contact the DPO to discuss if you are unsure whether you need to carry one out.

5.13 Transferring personal data to a country outside the EEA

Data Protection legislation impose strict controls on Personal Data being transferred outside the EEA. Transfer includes sending Personal Data outside the EEA but also includes storage of Personal Data or access to it outside the EEA. It needs to be thought about whenever the College appoints a supplier outside the EEA or the Institution appoints a supplier with group companies outside the EEA which may give access to the Personal Data to staff outside the EEA.

So that we can ensure we are compliant with Data Protection Laws College Personnel must not export Personal Data unless it has been approved by the Data Protection Officer.

All Personnel must not export any Personal Data outside the EEA without the approval of the Data Protection Officer.

6 Complaints

We are committed to a fully inclusive and transparent Data Protection Policy. Should you be dissatisfied with any aspect regarding data protection you can complain. Please refer to the Institution's Complaints Policy and Procedure for further information, which can be found in section 7 of this document.

7 Other relevant policies and procedures

- Lakes College – Higher Education Complaints Policy and Procedure

8 Any external references

- Competition Markets Authority Competition and Markets Authority - GOV.UK (www.gov.uk)
- Consumer Rights Consumer Rights Act 2015 (legislation.gov.uk)
- Data Protection Act (1997)
- Equality Act 2010 Equality Act 2010: guidance - GOV.UK (www.gov.uk)
- General Data Protection Regulation (2018)
- Office for Students Home - Office for Students
- Office for the Independent Adjudicator Office of the Independent Adjudicator for Higher Education - OIAHE
- The Open University Distance Learning Courses and Adult Education - The Open University
- Pearson Pearson | The world's learning company | UK
- University of Central Lancashire University of Central Lancashire - UCLan
- University of Cumbria University of Cumbria