

## **Lews Castle College UHI Data Protection Policy**

### **1 Introduction**

Lews Castle College UHI is committed to ensuring compliance with data protection legislation and good practice in exercising its responsibilities as a Data Controller.

Personal data will be processed in line with the seven key principles identified in the GDPR, namely:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

This policy sets out:

- The legislative context
- Systems and procedures
- Roles and responsibilities
- Rights of the data subject

### **2 Legislative Context**

The two main pieces of legislation relating to data protection are:

- General Data Protection Regulation (GDPR): European regulations that all member states must comply with, and that will continue to apply within the UK after Brexit; and
- Data Protection Act 2018 (DPA): adopts GDPR in its entirety and gives a framework for how the regulations will work specifically within the UK

This legislative context requires that personal data will 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, in accordance with Article 89(1), 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 will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is 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 is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation 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 will demonstrate its compliance with these principles.

### 3 Systems and Procedures

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. Other Privacy Notices are made available to individuals at the point where personal data is being gathered.

Privacy Notices are also available on the College website at <https://www.lews.uhi.ac.uk/about-us/privacy/privacy-notices/>

**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

Additional conditions apply if any special categories of personal data are being processed. Advice from the Data Protection Officer will be sought before any such processing commences. A Data Protection Impact Assessment may also be required.

**Data Sharing:** Data sharing arrangements including the basis for sharing will be detailed in the relevant Privacy Notice.

Where the College shares in the processing of personal data with a third party organisation, it will require that third party organisation to enter into a Data Sharing Agreement.

**Data Processing:** A data processor is a third party that processes personal data on behalf of the College (for example payroll, pensions). Data processing including the basis for this arrangement will be detailed in the relevant Privacy Notice.

Data processors must have appropriate technical security measures in place, maintain records of processing activities and notify the College if a data breach is suffered. A formal agreement of responsibilities will be agreed with any processor.

**Privacy Impact Assessment (PIA):** A PIA will be carried out before undertaking or processing activity which poses a high risk to an individual's privacy. The College will consult the Information Commissioner's Office in the event that a PIA identifies a high level of risk that cannot be reduced. The Data Protection Officer (DPO) will be responsible for this reporting.

**Retention:** The College will ensure that personal data is only retained for the necessary period of time. The College will ensure that all personal data is archived and destroyed in accordance within the period specified in the Retention Schedule. The Retention Schedule is published online here: <https://www.lews.uhi.ac.uk/t4-media/one-web/lews/about-us/publications/LCCRMPJuly2017.pdf>

**Breach Response:** The College is required to notify the Information Commissioner of any breaches of data protection which may cause harm. All breaches should be drawn to the attention of the Data Protection Officer as soon as they are known.

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.

**ICO Registration:** Lews Castle College UHI is registered as a Data Controller with the Information Commissioner, registration number Z7329015.

#### **4 Roles and Responsibilities**

**The Data Controller** has overall responsibility for setting the Data Protection Policy and outlining expectations of staff with regard to data protection. The Data Controller is the Principal, Sue Macfarlane, email: [sue.macfarlane@uhi.ac.uk](mailto:sue.macfarlane@uhi.ac.uk)

**The Data Protection Officer (DPO)** is responsible for providing information and advice to staff on data protection compliance and for monitoring the College's compliance with legislation and its policies. The DPO is also the main point of contact between the College and the Information Commissioner's Office on all matters related to data protection.

The DPO is James Nock, email: [dataprotectionofficer@uhi.ac.uk](mailto:dataprotectionofficer@uhi.ac.uk)

The DPO service is provided through Universities and Colleges Shared Services, offering access to a team of professionals if the named DPO is absent.

**The Board of Management** is responsible for oversight of arrangements to ensure compliance with data protection legislation.

**The Principal** has responsibility for allocating resources to ensure the effective administration of procedures and processes associated with data protection, including:

- Preparing and communicating Privacy Notices;
- Responding to Subject Access Requests;
- Supporting processes for Privacy by Design and Privacy Impact Assessments;
- Maintaining and updating relevant policies and procedures

**Managers** are responsible for ensuring that all personal data being processed within their area of responsibility complies with legislation and College procedures, seeking advice as appropriate from the DPO. They should ensure that staff within their Department have completed the relevant training and have the required levels of knowledge of data protection and related issues in order to fulfil their roles.

**The Staff Development Officer** is responsible for reviewing staff awareness of GDPR requirements and will arrange suitable training opportunities and monitor compliance with mandatory training modules.

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

All staff who are involved in processing data have a duty of care to ensure that data is processed in accordance with 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.

## **5 Rights of the Data Subject**

GDPR gives individuals specific rights, including the:

- 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
- Right not to be subject to automated decision making or profiling

Information on how to make a Subject Access Request, and how to make a complaint, will be publicised clearly. This information will be included in relevant documentation, and set out on the relevant pages on the website.

These arrangements are as follows:

**Subject Access Request:** If you wish to make a Subject Access Request please contact the Freedom of Information officer (email [lefoi@uhi.ac.uk](mailto:lefoi@uhi.ac.uk) or 01851 770000) who will provide you with the personal information which the College holds on you. Information will be provided within one month of the date of receipt of the request.

If you wish to exercise other rights please contact the Data Protection Officer [dataprotectionofficer@uhi.ac.uk](mailto:dataprotectionofficer@uhi.ac.uk)

**Complaints:** If you believe your personal data has not been processed in accordance with data protection legislation, you have a right to make a complaint to the Information Commissioner's Office. You can find details of how to make a complaint at <https://ico.org.uk/make-a-complaint/>

Approved by the Board: September 2018  
Review date: September 2020