Data Protection Policy

September 2022

Author: Data Protection Officer

Date: September 2022

Review Date: September 2025

Equality Impact Assessment Date: September 2022

Contents

History of Changes

Version No	Date of Approval	Approving Authority	Brief Description of Amendment
1.0	N/A		Initial Draft by Alice Wilson
1.1	March 2019		2nd Draft by Alice Wilson and Colin Miller
2.0	September 2022		Review by Lizi Bird, DPO, to make policy more concise; corrections to contact details; and update of data protection legislation.

West Lothian College is an inclusive organisation and all policies, procedures, strategies, plans, provisions, criteria, functions, practices and activities, including decisions and the delivery of services are assessed to consider the impact on staff and students covered by the Equalities Act 2010 by the completion of an Equalities Impact Assessment (EIA). Protected characteristics are defined as age, disability, gender reassignment, marriage or civil partnership (in employment only), pregnancy and maternity, race, religion or belief, sex, sexual orientation. All college policies and procedures can be provided in an accessible format.

1 Introduction

This is West Lothian College's Data Protection Policy. It sets out the legal framework, which govern our use of personal data; the college's commitment to protecting its personal data; and the obligations of users to protect personal data, with particular reference to special categories of personal data ('sensitive personal data').

It applies to all managers, employees, contractors, and anyone else who can access or use personal data in their work for the college.

It should be read in conjunction with the college's IT Security Policy, Email and Computer Network Responsible Use Policy, Social Network and Internet Policy, Staff IT Acceptable Use Policy.

Any concerns about the protection of data at West Lothian College ('the College'), or non-compliance with this policy, must be reported to GDPR@west-lothian.ac.uk

2 Purpose

At West Lothian College we create, collect, store and process large amounts of information; this includes personal and special categories of personal data, which are subject to data protection law.

The college is committed to protecting the confidentiality, integrity and availability of all information on the basis of its intrinsic value and risk. In this policy the college confirms its commitment to protecting *personal data*, and to protecting the rights and freedoms of individuals with respect to the processing of their personal data.

This policy, and associated policies and procedures, sets out data users' roles and obligations in protecting personal data, support the college's compliance with its obligations as a Data Controller (and where applicable, a Data Processor), under data protection law; and in managing risks to college data.

3 Scope

This policy applies to:

- All personal data created or received in the course of college business in all formats, of any age. "Personal Data" shall include personal and special category data.
- Personal data held or transmitted in physical (including paper) and electronic formats.
- Personal 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 personal 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 Governors and 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 personal data is accessed, including home access and overseas.

4 Objectives

This policy sets out a framework of governance and accountability for data protection compliance across the college and the college's responsibilities for this under data protection legislation.

The Data Protection Policy forms part of the college's framework for Information Governance more broadly and should be read in conjunction with associated policies and procedures.

5 Legal governance

The safe and secure management of personal data is integral to West Lothian College's values and a key enabler of effective business practice.

Beyond this, the college must comply with data protection legislation including UK General Data Protection Regulation; and UK Data Protection Act 2018 and Privacy and Electronic Communications Regulations (PECR).

These data protection laws require the college to protect personal data and control how it is used in accordance with the legal privacy rights of data subjects – the individuals whose personal data is held.

5.1 Data Protection Principles

Under data protection laws the college is responsible for, and must be able to demonstrate compliance with, the following data protection principles. There are 6 principles.

5.1.1 Principle 1: Personal data shall be processed fairly, lawfully and transparently.

This means West Lothian College will:

- Only collect and use personal data in accordance with the lawful conditions set down in data protection law and not breach any other laws;
- Treat people fairly by using their personal data for specific purposes and in a way that they would reasonably expect;
- Inform people how we use their personal data and what their rights are (known as a privacy notice). This includes being clear, open and honest about how the college uses their data to meet the transparency requirements of the right to be informed (see also section about individuals' rights);
- Rely on an individual's consent, as the legal basis for processing their personal data, only where:

    - We've obtained their specific, informed and freely given consent, and
    - They I have given consent, by a statement or a clear affirmative action (that we document); and
    - They have the right to withdraw their consent at any time without detriment to their interests; and that it is as easy to withdraw consent as it is to provide it.

5.1.2 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 West Lothian College will:

- Ensure that if we collect someone's personal data for one purpose (e.g., collecting a student's personal email address to correspond with them about an application for a programme of study), we will not reuse their 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);
- Be clear in the privacy notice as to the specific purposes of processing and ensure that the data subjects are fully informed (see also section on individuals' rights);
- If the data is to be used for another purpose ensure it is compatible with original purpose or get the individual's specific consent for the new purpose.

5.1.3 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 West Lothian College will:

- Only collect personal data sufficient and relevant for the stated purpose;
- Only collect the minimum data required, (i.e., we will not collect personal data 'just in case');
- Reduce risks of disclosure by pseudonymising personal data where possible;
- Anonymise personal data wherever necessary and appropriate, (e.g., when using it for statistical purposes), so individuals can no longer be identified;
- Review the data we hold and where appropriate delete what we do not need.

5.1.4 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 West Lothian College will:

- Take all reasonable steps to ensure personal data is not incorrect and have processes in place to ensure incorrect or misleading data is corrected 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);
- Ensure the accuracy of the personal data we create and record the source of that data (e.g., from data subject or from partner organisation);
- Have processes in place to address an individual's right to rectification; how it is considered, actioned, and recorded.

5.1.5 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 West Lothian College will:

- Only keep personal data for as long as necessary for the purpose it was collected for;
- Regularly review the retention period for any records containing personal data;

- Have appropriate processes in place to comply with individuals' requests for erasure under the 'right to be forgotten';
- Destroy personal data securely in a manner appropriate to their format or anonymise the personal data when we no longer require it;
- Identify personal data that needs to be kept for public interest archiving, scientific or historical research or statistical purposes.

5.1.6 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').

Principle 6, known as the Security principle, is about maintaining the confidentiality, integrity and availability') of personal data and the systems in which it is processed.

- Confidentiality: protecting from unauthorised access and disclosure;
- Integrity: safeguarding accuracy and completeness and preventing unauthorised amendment or deletion;
- Availability: ensuring information and associated services are available to authorised users whenever and wherever required;
- Resilience: the ability to restore the availability and access to information, processing systems and services in a timely manner in the event of a physical or technical incident.

This means West Lothian College will:

- Have appropriate organisational security measures in place to protect the confidentiality, integrity and availability of personal data (including policies, procedures and training);
- Have appropriate technical security measures in place to protect the confidentiality, integrity and availability of personal data;
- Have appropriate physical and personnel security measures in place, (e.g. secure rooms where personal data is held);
- Control access to personal data so staff, contractors and other people working in the college can only see the personal data 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;
- Set and monitor compliance with security standards for the management of personal data as part of the college's framework of information governance policies and procedures;

- Provide appropriate tools for staff, contractors, students and others to use and communicate personal data securely when working away from the college;
- Put in place appropriate agreements and auditable security controls where transferring personal data to another country outside the UK or European Union to maintain privacy rights;
- Have a robust security incident reporting procedure in place to manage, investigate and, where applicable, report to the Information Commissioner's Office and data subjects affected;
- Ensure the resilience of personal data processing systems and services, including the ability to continue to operate under adverse conditions (e.g. physical or technical incident); and ensure the college has the ability to restore these systems to an effective state.

In addition, the following apply at all times:

- All college users of data must ensure all data, and specifically personal and special category data, they hold is kept securely;
- Users must ensure personal 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 will be locked away when not in use; Portable devices (laptops, memory sticks, external hard drives) will not be left unattended.

5.1.7 Accountability

West Lothian College must also meet 'Accountability' requirements by adopting policies and implementing appropriate measures to ensure and demonstrate the processing of personal data complies with privacy law and the six principles above.

This includes the following:

- Records of Processing Activities. This will contain all the business functions of the college which collect personal data; the types of personal data collected; the source of the data; who (if any) it is shared with; the security measures in place to protect it; the retention and disposal of the data; the lawful basis it is collected for and the conditions for processing. This must be maintained and reviewed on a regular basis;
- Adopting and implementing data protection policies and procedures that demonstrate appropriate technical and organisational security measures are in place;
- Appointing a Data Protection Officer (DPO): the College DPO can be contacted through the Data Protection mailbox GDPR@west-lothian.ac.uk

- Implementing a ‘data protection by design and default’ approach. This means whenever a policy, process or system involves personal data, the college considers and builds appropriate safeguards to protect the personal data from the start;
- Use proportionate privacy and information risk assessment, and where appropriate data protection impact assessment, to identify and mitigate privacy risks at each stage of every project or initiative involving processing personal data; and in managing upgrades or enhancements to systems and processes used to process personal data;
- Ensuring appropriate contracts are in place with any third-party organisations who process personal data on the college’s behalf and where the college shares personal data with other organisations that this is properly documented in a data sharing agreement (DSA);
- Recording and where appropriate reporting personal data breaches to the regulator (UK Information Commissioner’s Office (ICO)) and if necessary, the data subjects;
- The college will adhere to relevant codes of conduct and where applicable sign up to certification schemes.

The accountability principle is an ongoing obligation; the college will regularly review (and where necessary update) documentation and risk assessments.

5.2 Rights of Data Subjects (Individuals)

Individuals (data subjects) have a number of rights under data protection law. These rights are explained in detail below.

Some rights have certain conditions that must be met for the rights to apply. Requests from those exercising their rights should be sent to GDPR@west-lothian.ac.uk to be processed accordingly. Primarily, requests must be answered within one month.

5.2.1 Right to be informed

This means, at the point we collect individuals’ personal data, we will explain to them in a clear, concise and accessible way through a ‘Privacy Notice’ how we use their information; as a minimum, this will include:

- who we are;
- why we use their information;
- who it is shared with;
- if it is sent outside of the UK;
- how they can get in touch with us; and
- how they can exercise their rights.

We will review the content of these Privacy Notices regularly and inform our data subjects of any significant changes that may affect them.

Where we process personal data for marketing purposes to keep people informed about college activities and events, we will provide in each communication a simple way of withdrawing their consent to of further marketing communications.

5.2.2 The right of access

Individuals have the right to request access to and receive a copy of their personal data, held by the college, free of charge.

5.2.3 Right to rectification

Individuals have the right to request to have inaccurate personal data rectified and incomplete personal data completed. We will also provide simple and secure ways for our students, staff and other data subjects to update the information that we hold about them, such as home addresses.

5.2.4 The right to erasure

This is commonly known as the right to be forgotten. It means individuals can have their personal data erased when it is no longer needed, if the data has been unlawfully processed or if the data subject withdraws their consent, unless there is an overriding legal or public interest in continuing to process the data.

5.2.5 The right to restrict processing

Individuals may restrict the processing of their personal data until a dispute about the data's accuracy or use has been resolved, or when the college no longer needs to keep personal data, but the data subject needs the data for a legal claim.

5.2.6 The right to data portability

In some circumstances, and where a data subject has provided personal data to the college by consent or contract for automated processing, they have the right to request a machine-readable copy or have it sent to another data controller.

5.2.7 The right to object

All individuals have the right to object and prevent further processing of their data in certain circumstances, including where the college is:

- Processing personal data for direct marketing
- Processing data obtained for online services such as social media, where consent for the processing was previously given by or on behalf of a child, who withdraws their consent;
- Making a decision about them solely by automated means;
- Carrying out processing in the course of the the college's legitimate interest or public interest unless the college can demonstrate compelling lawful grounds for continuing to process the individual's data.

5.2.8 Rights in relation to automated decision making and profiling

Automated decision-making means a decision is made solely by automated means and without any human intervention. Profiling is automating processing of personal data to evaluate certain aspects about an individual. This type of decision making can only be carried out where the decision is necessary for the entry into or performance of a contract; authorised by law or based on the individual's explicit consent.

When the college processes personal data which involves automated decision making or profiling the college will:

- Provide the individual with information about the processing;
- Provide a simple way for them to request human intervention or challenge a decision;
- Carry out checks to ensure that the systems are working properly as intended.

6 Risks of Non-Compliance

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. It is important to note,in the event of a personal data breach, individuals may claim compensation for damages caused by the breach.

Non-compliance with the data protection principles, or any concerns over data protection, must immediately be reported to, GDPR@west-lothian.ac.uk

7 Lines of Responsibilities

7.1 All users of college information are responsible for:

- Following policies and procedures and completing relevant training and awareness activities provided by the college to support compliance with this policy;
- Taking all necessary steps to ensure that no breaches of information security result from their actions (taking into account personal data security principles in 5.1.6);
- Reporting all suspected personal data breaches or incidents immediately to, GDPR@west-lothian.ac.uk so appropriate action can be taken to minimise harm;
- Taking all necessary steps to immediately limit and contain any damage to individuals which may, or has, resulted from a personal data breach;
- Complying with the data protection principles set out in in section 5;
- Informing the college of any changes to the information that they have provided in connection with their employment or studies, for instance, changes of address or bank account details.

7.2 The Principal and Chief Executive

As the Chief Executive Officer of the College, the Principal has ultimate accountability for the college's compliance with data protection law.

7.3 Vice Principal, Finance and Corporate Services

The Vice Principal, Finance and Corporate Services has senior management accountability for data protection, reporting to the Principal and Chief Executive and the Audit Committee on relevant risks and issues.

7.4 Data Protection Officer (DPO)

The Data Protection Officer (DPO) is independently appointed and part of a shared service. In line with the duties set out under data protection law, the (DPO) will support the college in its compliance with data protection law through the provision of independent advice and guidance; supporting the college to monitor internal compliance; providing advice regarding data protection impact assessments, and by acting as the first point of contact for data subjects and the Information Commissioner's Office (ICO).

In relation to personal data breaches and incidents, the college will consult with the DPO, who shall make recommendations to the college with specific regard to a). whether to report a personal breach to the regulatory body (ICO); b). whether to report a personal data breach to the affected individual(s); and c). recommendations for further actions and preventative measures

7.5 College Managers

College Managers are responsible for ensuring that all staff manage their devolved responsibilities for compliance with this policy.

8 Policy Monitoring and Evaluation

The terms of this policy must be observed at all times. Any failure to comply with the terms of this policy may lead to disciplinary action being taken against the user in accordance with the college disciplinary policy.

9 Related Policies, Procedures and Further Reference

This policy should also be read in conjunction with the College's Disciplinary policies and procedures as well as the policies detailed in Section 1.

These policies and procedures are reviewed and updated as necessary to maintain an effective Information Governance Management System to meet the College's business needs and legal obligations.

10 Further Help and Advice

For further information and advice about this policy contact: GDPR@west-lothian.ac.uk

11 Annex A – Definitions in Data Protection

The following provides a definition of the terminology used in this policy in relation to data protection law.

Availability means ensuring personal data and associated services are available to authorised users whenever and wherever required.

Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person such as facial images or dactyloscopic data (fingerprint).

Confidentiality means protecting personal data from unauthorised access and disclosure.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them.

Data concerning health means personal data related to the physical or mental health of a person, including the provision of health care services, which reveal information about an individual's health status.

Data Controller means the organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor means the organisation which processes personal data on behalf of the data controller. A data processor is subject to specific legal obligations; for example, maintaining records of personal data and processing activities and liability if responsible for a breach.

Filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample form the natural person in question.

Integrity means safeguarding the accuracy and completeness of personal data and preventing its unauthorised amendment or deletion.

Personal data means any information relating to an identifiable person (data subject); who can be directly or indirectly identified in particular by reference to an identifier. This definition is wide and means that a wide range of personal identifiers constitute personal data. This includes name, identification number

(e.g. NI Number), location data, online identifier (IP address) It also includes information relating to factors specific to the physical, physiological genetic, mental, economic, cultural or social identity of that individual.

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data. Processing occurs whether it is electronic or physical records, it includes: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. So even if data is held in a server but not used this is still processing.

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be identifiable without the use of additional information (e.g., use of key code). The additional information is kept separately and is subject to technical and organisational measures.

Recipient means a person, public authority agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; this processing by public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Resilience means the ability to restore the availability and access to personal data, processing systems and services in a timely manner in the event of a physical or technical incident.

Restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future.

Special category data (formerly known as sensitive personal data) means personal data which identifies an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life or sexual orientation. This data requires extra safeguards to protect it from unauthorised use, disclosure etc as it is considered that this information can have a higher impact on the rights and freedoms of an individual. Criminal records and convictions information is not

under this category of data but should also be handled with extra safeguards due to the sensitivity of the information.

Territorial Scope Data protection law applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

Third party means a natural or legal person, public authority, agency or boy other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data; (Art4(10)).

12 Equality Impact Assessment

Policy/Practice (name or brief description):	**Data Protection Policy**
Reason for Equality Impact Asessment (choose from the following options):	
• Proposed change to an existing policy/practice	• Review of existing policy
Person responsible for the policy area or practice:	
Name: Job title:	Lizi Bird Data Protection Officer
An Equality Impact Assessment must be carried out if the policy/practice: • affects **operational** or **strategic functions** of the College • is relevant to the promotion of equality (in terms of the Public Sector Equality Duty 'needs' as set out in the Policy and Guidance)	
Why the EIA is being carried out	The policy affects operational functions of the college.

Equality Groups Relevant to the Policy/Practice, identify which of the undernoted equality groups are impacted upon:	
• Age • Disability • race (including ethnicity and nationality) • religion or belief • sex • sexual orientation • gender reassignment • pregnancy and maternity • marriage or civil partnership	All as listed.

Record your assessment against the following statements:

Statement	**Equality assessment**
Detail the evidence of the needs of the identified equality groups and any gaps in information	The policy is in place to protect individuals' data. This applies to all groups of people.
Will application of this policy/practice lead to discrimination (direct or indirect), harassment, victimisation, less favourable treatment for particular equality groups?	No
If yes, how will the policy/practice be changed to contribute to advancing equality of opportunity	
State how this policy/practice will foster good relations:	Good relations with staff and learners will be formed since the policy aligns with current legislation, and is fair to all.
Will the policy/practice create any barriers for any other groups?	No
If yes, how will the policy/practice be changed to contribute to advancing equality of opportunity	
Which equality groups or communities have been consulted in the development and review of this policy/practice?	Consultation with Executive Leadership Team.

Equality Impact Assessment Outcome Select one of the four options below to indicate how the development/review of the policy/practice will be progressed and state the rationale for the decision. (Delete the options that do not apply):	
Option 1: No change required – the assessment is that the policy/practice is/will be robust.	**Option 1:** No change required – the assessment is that the policy/practice is/will be robust.
Monitoring	
When will the policy/practice next be reviewed?	September 2025
Publication of EIA	
Can this EIA be published in full, now? Please state Yes or No If No – please specify when it may be published or indicate restrictions that apply:	Yes
Sign-off	
EIA undertaken by Name: Jennifer McLaren Date: September 2025 Accepted by person responsible for the policy/practice named above: Name: Lizi Bird Date: September 2025	