General Data Protection Policy

Document History			
Author	Ian Grice	**Ref and Document Version**	GDPR_V6_IG230923
Reviewed by	Ian Grice	**Reviewed Date**	23/09/2023
Approval	Board of Trustees	**Approval Date**	06/10/2025
Next Review Date	31/07/2027	**Policy Number**	PRJ-20
Publication	Reception; Websites R:/Policies/General Data Protection Policy.pdf		

1 Approval and Review

1.1 This policy will be reviewed on an annual basis.

2 Policy Owner

2.1 The owner of this policy is the incumbent Data Protection Officer (DPO).

3 Purpose

3.1 An organisation which controls processing activities, involving Personal or Sensitive Data relating to European Union Data Subjects, must comply with the General Data Protection Regulation 2016 ('GDPR') and the Privacy & Electronic Communications Regulation 2003 ('PECR'). This policy sets out the requirements which all those in scope must adhere to.

3.2 This policy is subject to all the laws, rules and regulations that this organisation is governed by. In the event this policy allows the exercise of discretion, such discretion must be exercised within the confines of the organisation's statutory obligations and must not contravene any of its legal, accounting or other regulatory requirements.

4 Risk Appetite Statement

4.1 The Board of Governors of Management's Risk Appetite for a material breach of GDPR compliance is **LOW**.

4.2 The Board of Governors has identified personal data breaches, failure to uphold Data Subjects' rights and reputational damage as key data protection risks.

5 Glossary of Terms

5.1 A glossary of defined terms shall be included in Appendix A to this Policy.

6 Scope

6.1 The scope of this policy covers all Processing activities and supporting Information Systems involving Personal or Sensitive Data where the organisation acts as the

Controller. This includes personal, or sensitive data in physical form, stored in a relevant filing system.

6.2 The scope of this policy covers all global geographic territories. For the avoidance of doubt, this includes Third Countries, outside the European Union (EU).

6.3 The scope of this policy covers all Employees, Contractors, Third Parties, Processors or others who process Personal or Sensitive Data on behalf of the organisation.

7 Principles

7.1 Greenbank is committed to processing data in accordance with its responsibilities under GDPR. All processing activities shall be:

- Collected for specified, explicit and legitimate purposes only
- Accurate and, where necessary, kept up to date
- Retained only for as long as necessary
- Processed lawfully, fairly and in a transparent manner
- Processed securely, in an appropriate manner to maintain security
- Adequate, relevant and limited to what is necessary

8 Data Protection Officer (DPO)

8.1 A Data Protection Officer (DPO) shall be appointed and report directly to the Senior Leadership Team (SLT).

8.2 The DPO shall support the organisation in upholding the rights of Data Subjects as it relates to the organisation's processing activities.

8.3 The DPO shall respond to enquiries from Data Subjects in a timely manner.

8.4 The DPO shall establish and maintain a programme to monitor compliance with this policy.

8.5 The DPO shall establish and maintain a General Data Protection training and awareness programme.

8.6 The DPO shall support compliance with this policy by providing support and advice as it relates to complying with the requirements of this policy.

8.7 The DPO shall be provided timely and appropriate access to information and information systems as it relates to the discharge of their duties.

8.8 Details of the DPO, and the contact details shall be made publically available.

8.9 The DPO shall maintain the following registers:

- Register of Processing Activities
- Register of Data Protection Impact Assessments (DPIA)
- Register for Data Protection Metrics
- Register for Data Subject Enquiries

8.10 The DPO shall report personal data breaches to the Supervisory Authority no later than 72 hours after the breach has been detected.

9 Accountability

9.1 A record of processing activities shall be generated by the Data Protection Officer.

9.2 A System Owner shall be appointed for all Information Systems containing Personal or Sensitive Data. The System Owner shall **not** be from IT unless IT is performing the primary processing activity.

9.3 System Ownership shall **not** be assigned to a person who does not have budgetary responsibility of the Information System.

9.4 System Ownership shall **not** be assigned to a person who does not hold formal authority over those carrying out processing activities within the Information System.

9.5 A System Owner may delegate responsibility for operational tasks relating to the policy but shall not delegate accountability.

9.6 A System Owner may seek advice in the discharge of their duties but remain accountable for any subsequent decisions taken (e.g. acceptance of risk).

9.7 Processing activities must be documented and a Process Owner appointed.

9.8 Process Ownership shall not be assigned to a person who does not hold formal authority over those carrying out processing activity within the Information System.

10 Lawfulness of Processing

10.1 Process Owners shall ensure processing is lawful and document the lawful grounds for processing.

10.2 Where processing involves data of children, parental consent must be sought, provided and documented.

10.3 With the exception of storage, processing shall cease immediately where there are no longer lawful grounds for processing.

11 Transparency

11.1 Process Owners shall ensure information related to their processing activities is made available to the DPO so that an organisational Data Protection Privacy Notice may be published.

11.2 Data Subjects shall be informed of processing activities and will be provided statutory information at the time data is collected.

11.3 Where data is collected for a source other than the Data Subject, they shall be informed of processing activities and provided statutory information as soon as practical, but no less than 10 working days.

11.4 Process owners shall review the published Data Protection notice quarterly for any inaccuracies relating to their processes. The process owner shall report inaccuracies to the DPO within 5 working days.

12 Data Protection by Design & Default

12.1 Information systems and processes shall be designed to comply with the requirements of this priority.

12.2 Process and System Owners shall implement appropriate technical and organisational measures to ensure that data protection is stored and for the minimum period necessary.

12.3 Data protection and shall be integrated into all policies and procedures thereby informing production of required documentation such as Privacy Notices, Records of Processing and Records of Personal Data Breaches.

12.4 All information systems shall ensure their systems undergo a Data Protection Impact analysis ((DPIA) which contains at a minimum:

- A systematic description of the envisaged processing operations and the purposes of the processing.
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes.
- An assessment of the risks to the rights and freedoms of data subjects.
- The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this policy taking into account the rights and legitimate interests of data subjects and other persons concerned.

12.4 The system owner shall consult with the DPO in relation to the completion of the DPIA.

12.5 The DPO shall, where the risk to Data Subjects' rights is deemed HIGH, consult with the Supervisory authority.

12.6 System Owners shall ensure systems are explicitly designed to minimise the impact involved in upholding Data Subjects rights.

12.7 Process owners shall ensure processes are explicitly designed to minimise the impact involved in upholding Data Subjects rights.

13 Security of Processing

13.1 System Owners shall be accountable for ensuring systems meet the minimum required standards for security, but not limited to:

- Identity and access management
- Patch and vulnerability management
- Change management
- Backup and restoration
- IT service continuity planning and testing
- Development and testing activities
- Security breach monitoring and detection

13.2 Information systems, containing personal or sensitive data, exposed to the internet or third party, shall be subject to an independent, risk-based penetration test to an agreed scope, no less than annually. System Owners shall ensure all issues identified are appropriately treated commensurate with the Board of Governor's risk appetite.

13.3 Personal Data Breaches shall be reported to the DPO as soon as possible but no later than 24 hours after detection.

13.4 Staff members who process personal data about students, staff, applicants, or other individuals must comply with the requirements of this policy. Staff members must ensure that (a) all personal data is kept securely, (b) nor personal data is disclosed either verbally or in writing to any unauthorised third party and (c) personal data is kept in accordance with Greenbank's retention schedule.

14 Accuracy of Processing

14.1 Process owners shall ensure data remains accurate and where inaccurate corrected as soon as possible but no later than 5 working days from when the data is reported and verified.

14.2 Process Owners of processes involving automated decision making or profiling, shall document an alternative manual process and ensure appropriate resources are trained to carry out the manual process if required.

14.3 A Data Subject shall have a right not to be subject to an automated decision or profiling. Process Owner shall ensure this right is respected except where statutory exemptions apply.

15 Retention

15.1 With the exception of data held under statutory exemptions, personal data shall not be retained any longer than necessary.

15.2 The DPO shall retain an Information Retention Schedule which lists organisational information types and approved retention periods. The schedules will be based on data type and ownership and consider business value and associated regulatory compliance mandates.

15.3 In particular, all ESFA/ESF documentation will be retained securely until at least 31st December 2030. Before any ESFA/ESF project documentation is destroyed, a check of the gov.uk website and/or the Managing Authority to ensure that it is safe to do so.

16 Data Subject Access

16.1 Greenbank shall ensure it has the appropriate processes and resources in place to comply with GDPR rules relating to individual data protection rights. Greenbank will assist individuals to exercise the following data protection rights:

- The right of access
- The right of rectification
- The right to erasure
- The right to restriction
- The right to object
- The right to data portability

If any request is received in relation to a data subject's rights, the request must be referred to the Data Protection Officer at dpo@greenbank.org.uk

16.2 Process owners shall ensure those processing data understand how to identify a Data Subject Access Request (SAR).

16.3 Data Subjects Access Requests (SARs) shall be recorded in a register owned by the DPO.

16.4 Data subject access requests shall be completed as soon as possible but no more than 30 calendar days.

16.5 Greenbank reserves the right to extend the period of compliance by a further two months where requests are complex or numerous; Greenbank must however inform the Data Subject within one month of receipt of request and explain why an extension is necessary.

16.6 Data Subject Access Requests (SARs) shall not incur a charge.

16.7 Data Subject Access Request shall be processed electronically if this is requested by the Data Subject.

16.8 Reasonable steps shall be taken to verify the identity of the Data Subject prior to providing access to their personal data.

16.9 System owners shall ensure appropriate resources is made available to support Data Subject Access Requests.

16.10 Reasonable steps shall be made to seek the permission of third parties prior to including their information within and access request. Where permission is not provided, the DPO shall be consulted to determine whether data should be provided or redacted.

16.11 Requested information shall be communicated to the Data Subject securely.

16.12 Requested information shall be provided in a commonly used format; unless it is considered impossible, or if it takes 'disproportionate effort', or if Data Subject agrees to see it in some other form, e.g. view on screen.

17 Third Party Processing

17.1 Processing activities shall not be outsourced to a third party without a binding written contract that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of Data Subjects and the obligations and rights of the Organisation.

17.2 Process Owners shall only use third-party Processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this policy and ensure the protection of the rights of the Data Subject.

17.3 Process and System Owners shall consult with, and attain a written recommendation from the DPO and representatives from Legal, Procurement, Information Security, Business Continuity and Risk prior to signing a contract with a third party Processor and with sufficient time to carry out effective due-diligence on the proposed outsourced process and the third party Processors data protection technical and organisational controls.

17.4 Process and System Owners shall engage an independent (internal or external) assessor that is professionally qualified to assess the third party Processor's data protection technical and organisations controls.

17.5 Process and System Owners engaging third-party Processors shall ensure continuing compliance with this policy and maintain accurate records of relevant meetings and

compliance visits including supporting in evidence of the third party Processor's ongoing compliance.

18 Roles and Responsibilities

18.1 The Board of Governors has overall responsibility for this policy, and for reviewing the effectiveness of actions taken in response to concerns raised in this policy.

18.2 The Senior Leadership Team shall ensure appropriate resources are made available to support the implementation of this policy throughout all in-scope areas.

18.3 All those in scope of this policy are responsible for adhering to the requirements of this policy

18.4 The Data Protection Officer (DPO) is responsible for monitoring compliance with this policy and shall provide periodic reporting to the Board of Governors and Senior Management on the organisation's compliance with this policy.

18.5 The Data Protection Officer (DPO) shall be the contact point for all matters relating to the Supervisory Authority (SA).

18.6 Those described as Owners of this policy are responsible for ensuring their Processes, and Information systems meet the minimum requirements of all in-scope policies.

18.7 The Owners of the policies, detailed in 10.1, shall ensure requirements are amended to reflect the requirements of this policy.

18.8 The Human Resources Department shall ensure Human Resources processing is compliant with the requirements of this policy.

18.9 The Marketing Department shall insure processing related to marketing activities is compliant with the requirements of this policy.

18.10 Those responsible for Procurements shall ensure procurement processes are compliant with the requirements of this policy.

18.11 Internal Audit shall provide the Board of Governors with independent assurance that the organisation is adhering to the requirements of this policy.

19 Compliance

19.1 Failure to comply with this procedure could result in action in line with Greenbank's Disciplinary Procedure or Capability Procedure.

19.2 Compliance checks will be undertaken by Greenbank's Information Governance functions. The results of compliance checks, their risk assessment and their remediation will be managed by the Information Governance Board.

20 Related Documents

20.1 This control procedure needs to be understood in the context of other policies and procedures constituting Greenbank's Information Security Management System. The following policies also include specific and supporting requirements:

- Information Security Policy
- Mobile Devices and Teleworking policy
- Access Control Policy
- Communications Security Policy

21 Review

21.1 A review of this policy will be undertaken by the Information Security Team annually or more frequently as required and will be approved by the Information Governance Board.

Appendix A - Glossary of Terms

Access
Access refers to any mechanisms by which individuals gain access to information.

Availability
Availability involves ensuring information and the associated services needed to process that information are available to staff and students when required.

Computer Software
Computer Software is the collection of computer programs used to process information.

Confidentiality
Confidentiality requires protection of information from unauthorised disclosure or intelligible interception (see below).

Data Controller
Data controller means a person who (either alone or jointly or in common with other persons) **determines the purposes for which and the manner in which** any personal data are, or are to be, processed.

Data Processor
Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Data Protection (DP) Principles
The General Data Protection Regulation (GDPR) 2016, sets out the Data Protection Principles. In summary these state that personal data should be:

I. processed lawfully, fairly and in a transparent manner,
II. collected for specified, explicit and legitimate purposes,
III. adequate, relevant and limited to what is necessary,
IV. accurate and where necessary kept up to date,
V. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed, and
VI. processed in a manner that ensures appropriate security of the personal data.
VII. Accountability is central to GDPR. Data controllers are responsible for compliance with the principles and must be able to demonstrate this to data subjects and the regulator.

Data Subject
Data subject means an individual who is the subject of personal data.

Integrity
Integrity involves safeguarding the accuracy, completeness and consistency of both information and computer software.

Information
Information for the purposes of this policy includes data stored on computers, transmitted across computer networks, printed, written, sent by post or fax, or stored on removable devices. The policy applies specifically to electronic information but the same principles apply to paper-based information. Information may be either structured according to some defined format, or unstructured.

Personal Data
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 provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifiers.

Processing
'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as 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.

Security
Security refers to mechanisms and procedures designed to ensure that appropriate controls on information access are in place and are effective.

Sensitive Personal Data

Sensitive personal data (or 'Special Category' data under the GDPR) means personal data consisting of information as to the Data Subject's

- racial or ethnic origin
- political opinions
- religious beliefs or philosophical beliefs
- a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- genetic data
- biometric data
- data concerning health
- sex life or sexual orientation

Subject Access Request (SAR)
"Subject access" is the right of an individual to access personal data relating to him or her which are held by the University.

Author: Ian Grice Document version: GDPR_V6_IG230923

Agreed by Greenbank Board of Trustees

Dr Alan Irving, Chairman