Data Protection Policy

1. Introduction

1.1. The Queen's Foundation recognises that the protection of data is a serious issue. The Foundation is committed to protecting the rights and freedoms of all individuals in relation to the control and processing of their personal data, in accordance with the duties required by the Data Protection Act 1998 and the General Data Protection Regulation 2018 (GDPR). This undertaking stands both where the Foundation is the data controller and in processes where it is the data controller.

1.2. The policy has been approved by the Governors of the Foundation. It will be overseen by the Principal, who is the Foundation's Data Protection lead, and managed by the Director of Operations.

2. Scope

2.1. This policy sets out the responsibilities of all who process data on behalf of the Foundation whether Governors, staff (including contractors and volunteers) or students.

2.2. Any use of the term 'staff' in this policy shall also be taken to include volunteers and contractors, as relevant.

2.3. The policy applies to all personal data handled by Queen's, whether that data is held in paper files or electronically. So long as the processing of the data is carried out for the purposes of Queen's, it also applies regardless of where data is held. This includes all data stored on any devices (including electronic notebooks or laptops), regardless of who owns the PC/device.

2.4. 'Processing' data includes any and every form of action taken in relation to the data such as obtaining, recording, keeping, or using it in any way; sharing or disclosing it; erasing and destroying it.

3. Definitions

3.1. The key terms which are used in the GDPR, and in this Data Protection Policy, can be found at *Appendix 1*.

4. Principles for Data Processing

4.1. Under the GDPR, the handling of personal data must be:

- Fair, legal and transparent
- Collected for a specific purpose and only used for that purpose
- Adequate, relevant, and limited to what is needed for the purpose of the collection
- Accurate and up-to-date
- Kept in a format where individuals can be identified only for as long as is necessary
- Kept secure and confidential

4.2. More information about what each principle means can be found at *Appendix 2.*

5. Legal Basis for Processing Data

5.1. Any person or organisation who handles personal data must have a valid legal basis for doing so. To be able to function as a charity and a provider of higher education, the Foundation needs to collect and keep certain types of information about the people with whom it deals.

5.2. The lawful grounds on which the Foundation processes data are:

5.2.1. For the performance of a contract (or negotiations to enter into a contract)
The Foundation must collect and process personal data to enable the delivery of programmes of study. This includes information relating to all applicants, students, staff, and Governors. Where someone refuses permission to allow the Foundation to process their data for the purposes of this legitimate business, it will not be possible for that person to participate in the educational activities.

As a charity, the Foundation also collects and processes personal data to further its legitimate interests in running events and conferences. This includes information relating to supporters, those who attend events, staff and volunteers, and Governors.

5.2.2. For the performance of a public task in the public interest
This applies where data is used to meet the Foundation's obligations and duties, for example in fulfilling the obligation to share data with the Higher Education Statistics Agency (HESA), the Office for Students, and external regulators.

5.2.3. Vital Interest
This means for the protection of life, for example, sharing information with the emergency services or welfare organisations if there is significant evidence to suggest that someone is in danger.

5.2.4. Legal obligations
This applies where the Foundation has been ordered by a court of law to disclose information or to meet financial reporting obligations.

5.2.5. Legitimate interests
This applies where the use of personal data is in the legitimate interests of the Foundation and where this use is not deemed to be intrusive or to put the individual at any risk and is for the purpose of delivering or improving services or investigating technical issues.

5.2.6. Consent
This applies when free, informed, and specific consent has been given.

5.3. The Foundation is entered on the Information Commissioner's Office (ICO) Register of Data Controllers. This registration, which is reviewed annually, contains full details of the basis on which the Foundation processes data, what type of information is included, and who it might be shared with.

6. Data Handling

6.1. Appendix *3* gives a summary of the Foundation's data collection, storage, and deletion practices.

7. Data Security

7.1. Keeping personal data secure is key in complying with the GDPR. All students, staff, and Governors are responsible for ensuring that any personal data they have access to is kept securely and is not disclosed to any unauthorised third party, whether deliberately or accidentally, either orally or in writing.

7.2. Data protection training will form part of the Induction Programme for new staff and Governors, and refresher training will be carried out periodically.

7.3. A description of data security responsibilities can be found at *Appendix 4.*

8. Data Collection for Research Purposes

8.1. Students, staff, and any Governors at the Foundation who are involved in research may collect or create data and materials for the purpose of analysis to generate original research results. This may contain personal data and/or sensitive personal data. The data handling and security provisions of this policy will apply in all such cases and such considerations would form part of the research process's ethical review. Data subjects will also receive a privacy notice telling them how their data will be used and what options are available to them if they wish to enquire further.

8.2. Personal data obtained or used for research shall be limited to the minimum amount which is reasonably required to achieve the desired academic objectives and wherever possible any such personal data should be made anonymous so that the data subjects cannot be identified.

8.3. All students who are going to undertake research which involves handling personal data will be given specific guidance on data protection policy and practice.

9. Personal Data in the Public Domain

9.1. The Foundation holds certain information about Governors, staff, and students in the public domain. Personal data classified as being in the 'public domain' refers to information which will be publicly available world-wide and may be disclosed to third parties without recourse to the data subject.

9.2. The following items of data will be available:

- Foundation email addresses and telephone numbers for staff and Governors
- Foundation email addresses for students
- academic staff and Governor biographies where supplied
- names and academic qualifications of academic and support staff and Governors where appropriate

- any additional information relating to data subjects which they have agreed to be placed in the public domain and which may be in automated and/or manual form.

9.3. As part of regular business activities, the Foundation may process personal information about third parties which is already in the public domain. Such processing will be carried out in accordance with the GDPR principles set out in this policy.

10. Individual Rights

10.1. In compliance with the GDPR, the Foundation recognises that individuals have certain rights regarding their data. These are the right to:

- be informed about the collection and use of their personal data
- request access to the personal data which is held about them
- request rectification should an individual find that the data which the Foundation holds regarding them is inaccurate, misleading, or incomplete
- request erasure (also known as the right to be forgotten) should an individual wish to be removed from data records
- request restriction on processing
- data portability, allowing individuals to obtain their personal data so that they can reuse it for their own purposes
- object to their data being processed for direct marketing or for research and statistics.

10.2. All requests made under these rights must be referred to the Director of Operations.

10.3. The Foundation will keep a log of such requests in order to inform future improvements in how data is processed or held.

10.4. When a request is made:

- proof of identity will be required before personal data is released or erased
- all relevant data which the Foundation holds will be reviewed against the requirements of the GDPR for the grounds of the request and the individual will be notified of the outcome. The response will include information about their rights of appeal
- in most cases, the Foundation will fulfil the request within one month. However, in some circumstances (e.g., where requests are complex or numerous) this period may be extended by up to two more months. If this is the case, the Foundation will let the individual know why the extension is necessary within one month of the request
- in most cases, the Foundation will fulfil the request free of charge. However, in some circumstances (e.g., excessive or repetitive requests) there may be a charge
- where a request is unfounded, excessive, or repetitive, the Foundation may refuse the request.

10.5. Further details of these rights and how to exercise them may be found at *Appendix 5*.

11. Data Breaches

11.1. A personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Therefore, it covers breaches which are the result of both accidental and deliberate causes. It also means that a breach is about more than the loss of personal data.

11.2. If anyone believes that there has been a data breach, they should notify their line manager and contact the Director of Operations immediately.

11.3. The Director of Operations will investigate the source and nature of the breach and, if the security of personal data has been compromised, will establish what the likely impact will be on the individual(s) whose data it is.

11.4. If the likely impact is small, the Director of Operations will take steps to correct the situation which made the breach possible. If appropriate, the data subject(s) who are affected will be informed, and action will also be taken against the originator of the breach.

11.5. If the impact of the breach is of a severity that will put the rights and freedoms of those affected at risk, then the Director of Operations will notify the ICO in writing within the 72-hour statutory window and will also notify the data subject(s) affected.

12. Prohibited Activities

12.1. The following activities are strictly prohibited:

- using data obtained for one purpose for another supplemental purpose (for example, using contact details provided for HR-related purposes for marketing purposes)
- disclosing personal data to a third person outside of the Foundation without the consent of the data subject, except as required or permitted by statute
- retaining data past the point allowed by this policy 'just in case it might be needed.'

13. Compliance with this Policy

13.1. Compliance with the General Data Protection Regulation 2018 is without exception the responsibility of all students, staff, and Governors at the Foundation.

13.2. It is a condition of employment in the case of staff and enrolment in the case of students, that every individual abides by this policy, and any breach may lead to disciplinary action. A serious breach of the GDPR may also result in the Foundation and/or the individual being held liable in law.

14. Policy Review

14.1. This policy shall be reviewed annually, to ensure that it continues to meet the requirements of current Data Protection regulations and practice.

Any enquiries regarding this policy should be addressed to:

The Director of Operations
Email: dataprotection@queens.ac.uk
The Queen's Foundation for Ecumenical Theological Education
Somerset Road, Edgbaston, Birmingham B15 2QH
Tel: 0121 452 1527

Other Related Policies and Procedures:

Academic Freedom and Freedom of Speech
Academic Appeals
Academic Malpractice
Academic Progress Procedures
Acceptable ICT Use and ICT Guidance
Admissions Policies
Admission Complaints
Complaints Policy
Communication and Publicity Policy
Data Handling practice and procedures
Equality Policy
Fitness to Practice Framework
Fitness to Study Policy and Procedure
Harassment and Bullying Policy
Privacy Notices
Refund and compensation Policy
Recruitment Practice and Procedure
Safeguarding Policy
Staff Handbook and related procedures
Widening Participation

Appendix 1: GDPR Key terms

Data Controller is the organisation who determines the purpose and way in which data is being processed.

Data Processor is any person or organisation who processes data on behalf of the Data Controller.

Personal Data**:** is any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, from the data and any other information which is in the possession of, or likely to come into the possession of, the Foundation as the Data Controller.

It includes, but is not limited to:

- factual (eg, name, address or date of birth)
- Student ID number
- opinion (eg, performance appraisal)
- statement of intention about them
- 'online identifiers' such as computer IP addresses
- Info held in both electronic and paper format is covered

'Special Category Data', previously known as 'Sensitive Personal Data'.
This includes, but is not limited to, data regarding:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data
- data concerning health
- data concerning a natural person's sex life or sexual orientation.

Confidential data is data given in confidence or data agreed to be kept confidential between two parties, and that is not in the public domain. Some confidential data will also be personal data and/or sensitive personal data and will therefore come within the terms of this policy.

Processing means any operation performed on the data, for example: collecting, using, disclosing, retaining or disposing of personal data.

Personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Therefore, it covers breaches which are the result of both accidental and deliberate causes. It also means that a breach is about more than the loss of personal data.

Appendix 2: 6 KEY PRINCIPLES

The GDPR sets out the principles which data controllers must abide by when they are handling data about individuals, and they are as follows.

Lawfulness, fairness and transparency: personal data must be processed lawfully, fairly and in a transparent manner.

Purpose limitation: personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (with exceptions for public interest, scientific, historical or statistical purposes).

Data minimisation: personal data must be adequate, relevant and limited to what is necessary in relation to purposes for which they are processed.

Accuracy: personal data must be accurate and, where necessary, kept up to date. Inaccurate personal data should be corrected or deleted.

Retention: personal data should be kept in an identifiable format for no longer than is necessary (with exceptions for public interest, scientific, historical or statistical purposes).

Integrity and confidentiality: personal data must be kept securely.

Appendix 3: Data Handling

In accordance with the Foundation's entry to the ICO Register of Data Controllers, operating as a charity and a higher education organisation, the Foundation collects and processes data in the following ways.

Staff and Governors:
Data is collected at recruitment and then again at appointment.

- ***At recruitment***, the data will be supplied by applicants, in the form of application forms, or CVs and covering letters. This data will usually be collected and stored electronically. If the candidate has sent hard copies, these will be kept in a secure office. Data gathered during the appointment of new Governors will also be handled in this way.

  Candidate information for unsuccessful applicants will be deleted once an appointee has taken up the post, unless the Foundation has the candidate's specific permission to retain their details for a defined period in case another suitable vacancy comes up.

  For the candidate who is appointed, further details will be requested:
  - ID to prove legal right to work in the UK. An electronic copy will be kept for the duration of the employment/contract
  - Bank details to enable payment. These will be kept for the duration of the employment or contract and deleted when the employment/contract ends
  - CV from staff, a copy of which may be sent to the validating university. This will be kept for the duration of the employment/contract

- ***Appraisals:*** annual staff appraisals will be carried out following the Foundation's approved processes. Appraisal letters and forms which are agreed and signed off will be kept electronically for 7 years.

Staff data is processed and managed by the human resources financial services staff.

Data for Governors is processed and managed by appointed Governors, the Foundation Principal, and key appointed staff.

Applicants
Those who wish to study at the Foundation provide their details during the applications process.

They are asked to supply:
- Evidence of their right to study in the UK (except in the case of those who are applying to study solely by distance learning)
- Academic certificates to prove their eligibility to enrol to the course
- documents to support an enhanced DBS application as applicable
- passport-style photo for the purposes of an ID card

This information is held electronically and is uploaded to the applicant database during the admissions process.

Where a place is not offered, the applicant data is retained for 12 months after the last date of contact. For applicants to research programmes, data is retained for 24 months after the last date of contact.

Where a place is offered and accepted, the data is moved from the applicant database to the student database. Applicants who plan to make payments direct to the Foundation must also supply bank details.

Applicant Data is stored electronically, and may be processed by:

- Admissions staff
- Staff team of the programme applied for
- Finance team
- Data and IT team

Students

Where a place is offered and accepted, some students may require an enhanced DBS check. This may be carried out using the data and documents they have provided during the application process.

At enrolment, students are asked to complete a student data form gathering data required by HESA, and are given a data collection notice explaining why their data is collected and how it will be processed.

They are also asked to provide details of who the Foundation should contact in case of emergency.

During their course, data is kept regarding their studies. This includes assessments and any supporting data. Academic assessment information will be shared with the validating university as will photo ID for the production of ID cards.

The personal data is stored electronically and is kept for the duration of their course. For those who give their consent, their contact details may be added to the alumni or other specified database, where they will be securely retained unless the individual asks for them to be removed.

Data is stored electronically, and is processed by the:

- Staff of the programme applied for
- Finance staff
- Data and IT staff
- External examiners
- Hospitality and Services staff for accommodation matters
- Marketing staff where specific consent is given

Grade and Assessment information continues to be stored in perpetuity, available to the Foundation staff and representative as above, the individual and anyone authorised by the individual.

Events and Conferences

The Foundation as a charity and conference facility collects contact details for those who register for events, or otherwise express an interest in events and services being offered.

Data collection/Privacy notices are provided, so that individuals can confirm if and how they would like to be contacted in future.

Such data is stored electronically, and is processed by the:

- Marketing staff
- Programme staff as relevant

Historical Data

Historical data has been archived as follows:

- Hard copies of records are held in locked storage
- Electronic records are held in password-protected storage

Historical records will be reviewed as part of the ongoing administrative housekeeping process, so that previous data is only stored for as long as it is unavoidable to do so.

.

Appendix 4: Data Security

As a minimum, keeping personal data secure includes ensuring that:

- if any personal data is recorded in paper form or hard copy, the documents are kept in locked filing cabinets or locked drawers or in locked offices
- if any personal data is recorded to discs, memory sticks or electronic devices, these are protected by passwords
- if any personal data is held on a Mobile Device such as a laptop, the device is password protected

Responsibilities of staff, students

All Governors, staff and students must ensure that they only ever process or hold personal data in accordance with requirements of the GDPR and this Data Protection Policy. Everyone who processes any personal data for any purpose related to the Foundation must abide by the principles below.

1. Remain mindful that individuals have the right to see their 'personal data', which may include comments written about them in emails. Staff and students should not record comments or other data about individuals which they would not be comfortable for the individual to see, whether in emails or elsewhere.
2. Ensure that passwords and logins are not shared with unauthorised users.
3. Remain mindful that data which is held on remote devices is covered by this policy, regardless of who owns the device or where it is stored.
4. Ensure that if their laptop/mobile device has more than one user each has a separate, password-protected login.
5. Take special care when data is transferred from one place to another (for example, take care not to misplace laptop or memory sticks in transit).
6. Immediately notify their Line Manager and the Director of Operations if they find any lost or discarded item which they believe contains personal data, whether paper-based or otherwise.
7. Immediately notify their line manager and the Director of Operations if they become aware that personal data has been accidentally lost or stolen or inadvertently disclosed, for example if their laptop or other device is lost or stolen and has personal data stored on it.
8. Hold the contents of any personal data which comes into their possession securely.
9. Ensure that personal data (such as their contact details) which they provide to the Foundation is accurate.
10. Notify the relevant contact at the Foundation promptly if there are any changes to their personal data, for example a change of address or emergency contact details.
11. Only ever obtain or use personal data relating to third parties for approved work or study-related purposes.
12. Seek advice from the Director of Operations if any data protection related concerns arise.

Appendix 5: Individual Rights

In compliance with the GDPR, the Foundation recognises that individuals have certain rights regarding their data, detailed below.

If any member of staff receives a request under these rights, whether in writing or verbally, they must notify the Director of Operations immediately, so that the Foundation can meet statutory deadlines in processing the request.

The Individual rights are as follows:

- **Right to Be Informed** about the collection and use of their personal data.
  Where the Foundation has or may collect personal data, notices are provided at the point of collection to ensure that they are aware of the data which is being collected, the purpose it is being collected for, and how long it will be kept.

  These notices are:
  - Privacy Statement on the website
  - Student Data Collection Notice for the collection of HESA data
  - Research data privacy notice
  - Events & Direct Marketing consent forms
  - Job applicants: link to Data Protection Policy on the job advert
  - Data Protection Policy and information available on the website for all staff and other users

- **Right of Access** to the personal data which is held about them.
  - Individuals may exercise this right by completing the Subject Access Request form below and sending it to the Director of Operations.
  - Some data may be exempt from this right, for example, where the legal right of confidentiality applies.
  - Documents will normally be produced electronically, in PDF format. If this is not possible, a file of documents in hard copy will be produced and sent through the post.

- **Right of Rectification:** if an individual feels that the data which the Foundation holds about them is inaccurate, misleading, or incomplete, they can ask for it to be revised.
  - The request may be made verbally or in writing.
  - The Foundation will take reasonable steps to verify whether revision is justified, and notify the individual of the decision and any subsequent action.
  - If the decision is taken not to amend the data, the individual will receive an explanation of the reason, and of their right to appeal.
  - Where it is practical to do so, the Foundation will notify other organisations to whom they have supplied data which is rectified under this right.

- **Right of Erasure** (also known as the **'right to be forgotten'**): an individual may apply to have their data removed.
  - The request may be made verbally or in writing.

- This is not an absolute right and only applies in certain circumstances within the definition of the GDPR.
- Should the request be agreed, the Foundation will notify the individual of the decision and any subsequent action.
- If the Foundation does not agree the request, the individual will be informed of the reason, and of their right to appeal.
- Where it is practical to do so, the Foundation will notify other organisations to whom they have supplied data.

- **Right to restrict processing**: an individual may request the restriction or suppression of their personal data, where the Foundation will keep the data but not make use of it.
  - This is not an absolute right and only applies in certain circumstances within the definition of the GDPR, and the restriction may be time limited.
  - The request may be made verbally or in writing.
  - The Foundation will not process the data in question while the request for restriction is being processed.
  - Should the right to restriction be agreed, the Foundation will notify the individual of the decision and any subsequent action.
  - The restriction on processing may be for a limited time, in which case the individual will be notified before it is lifted.
  - If the Foundation does not agree the request, the individual will be informed of the reason, and of their right to appeal.
  - Where it is practical to do so, the Foundation will notify other organisations to whom they have supplied data.

- **Right of Data Portability**: allowing individuals to obtain their personal data so that they can reuse it for their own purposes.

- **Right to Object**: to their data being processed for direct marketing or for research and statistics.

Requests under these rights should be made to:

The Director of Operations
Email: dataprotection@queens.ac.uk

The Queen's Foundation for Ecumenical Theological Education
Somerset Road, Edgbaston, Birmingham B15 2QH
Tel: 0121 452 1527

Subject Access Request Form

Please provide the following information to help us give a timely and accurate response to your enquiry. Please send the completed form and any other documents to The Director of Operations, either by email to dataprotection@queens.ac.uk or by post to: The Queen's Foundation for Ecumenical Theological Education, Somerset Road, Edgbaston, Birmingham, B15 2QH

PART A *Please enter your details in* ***block capitals****:*

Surname:	Title
Forename(s):	ID number (if current student/staff):
Address: Postcode:	Telephone No(s): E-mail address:
Relationship to the Foundation: Student / Member of Staff / Graduate / Other (please specify)	
Please include copies of two forms of identification documentation, such as a birth certificate, passport or driving licence along with this request. Failure to provide this documentation may delay the progress of your request, as the Foundation will not release personal data unless fully satisfied as to your identity.	
REQUEST: **Please provide a clear description of the information that you are requesting, including, where possible, dates and/or any additional information which will enable us to locate it.**	
PART B *Declaration* *I am the data subject named in Part A of this document and hereby request The Queen's Foundation to provide me with a copy of personal information held about me under the provisions of the General Data Protection Regulation 2018*	
Signed	Date