**Data Protection Policy**

<table>
<thead>
<tr>
<th>Category:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td>Data Protection Policy</td>
</tr>
<tr>
<td>Approval:</td>
<td>Policy Advisory Group</td>
</tr>
<tr>
<td>Responsibility:</td>
<td>Hugh Horton, Vice Provost and Executive Director</td>
</tr>
<tr>
<td>Dates:</td>
<td>Approved: 16/09/2021</td>
</tr>
<tr>
<td></td>
<td>Last Revised: NA</td>
</tr>
</tbody>
</table>

**Definitions:**

<table>
<thead>
<tr>
<th>Term:</th>
<th>Meaning:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal data</td>
<td>Information that relates to an identified or identifiable individual (‘data subject’).</td>
</tr>
<tr>
<td>Special category personal data</td>
<td>Personal data which is more sensitive and needs greater protection. There are eight types of information cited in the legislation: race or ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life and sexual orientation.</td>
</tr>
<tr>
<td>Data controller</td>
<td>Determines the purposes and means of processing personal data.</td>
</tr>
<tr>
<td>Data processor</td>
<td>Responsible for processing personal data on behalf of a controller.</td>
</tr>
<tr>
<td>Processing</td>
<td>Any operation or set of operations that 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.</td>
</tr>
<tr>
<td>Data Subject</td>
<td>Identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.</td>
</tr>
<tr>
<td>Consent (of the data subject)</td>
<td>Any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.</td>
</tr>
<tr>
<td>Third party</td>
<td>A natural or legal person, public authority, agency or body 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.</td>
</tr>
<tr>
<td>Data breach</td>
<td>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</td>
</tr>
</tbody>
</table>

The full list of definitions is available at [https://gdpr-info.eu/art-4-gdpr/](https://gdpr-info.eu/art-4-gdpr/).

**Purpose:**

The BISC recognises that compliance with UK data protection law is essential, and this policy details the BISC’s obligations under, and commitment to, data protection.

**Legislative Framework:**

The UK data protection framework is set out in the Data Protection Act 2018 (replacing the DPA 1998) and the UK GDPR, which came into force on 1 January 2021 and sets out the key principles, rights and obligations for the processing of personal data in the UK.

**Scope:**

This policy applies to all staff and faculty at the BISC who obtain, store, and process personal data.
Responsibilities under the policy

As data controller, the BISC is institutionally responsible for compliance with UK data protection law and must also maintain evidence of such compliance. Here are the levels of compliance that must be adhered to.

The Data Protection Officer is responsible for the application of data protection law at the BISC. They will:

- advise the BISC of its obligations;
- monitor compliance with the policy, including providing employees with training and raising awareness;
- ensure the provision of procedures, guidance, and advice in support of the policy;
- act as the first point of contact with the Information Commissioner’s Office (ICO);
- direct the completion of Subject Access Requests;
- investigate losses and unauthorised disclosures of personal data.

Managers and departmental leads are responsible for

- ensuring that their team is aware of data protection principles and are compliant with this policy and any supporting guidance and procedures;
- ensuring that the third-party vendor services used by their team comply with data protection law.

All employees are responsible for:

- complying with this policy and any supporting guidance and procedures;
- processing personal data in accordance with data protection principles as set out in this policy;
- passing on to the DPO any individual requests submitted as part of the ‘rights of the data subject’ as set out in this policy;
- support the DPO by responding within agreed timescales to requests for data in support of investigations and subject access requests;
- reporting to the DPO data security incidents, losses, near misses, or unauthorised disclosures and supporting the DPO in the follow-up investigations.

Compliance with the data protection principles

The BISC is committed to complying with the data protection principles, the first six of which relate to data processing and the seventh of which relates to the role of the data controller. We ensure that data is:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals (‘lawfulness, fairness and transparency’).
2. Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes (‘purpose limitation’).
3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’).
4. Accurate and, where necessary, kept up to date (‘accuracy’).
5. 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’).
6. 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’).
7. Processed in such a way that the BISC is responsible for, and able to demonstrate compliance with, the above principles (‘accountability’).

Data subject rights

The BISC is committed to upholding the rights of individuals as defined by data protection law.

- The right to be informed: we make explicit in plain language what data we collect, how we use it and how it is kept.
- The right of access: we provide copies of personal data to individuals who make a subject access request. We provide data within one month free of charge, unless the request is manifestly unfounded, repetitive, or excessive.
- The right to rectification: we update inaccurate information upon request and within one month of the request being made.
- The right to erasure: we delete the data of individuals where the data held is no longer required, where it was unlawfully processed, or where it no longer meets the lawful ground upon which it was obtained. We will delete the data of individuals upon request where one of these conditions is met, or where consent to process data has been withdrawn, except where we have a lawful ground to process data.
- The right to restrict processing: we restrict the use of personal data upon request while we determine our legal ground to process the data obtained.
- The right to data portability: we provide personal data to the data subject upon request for data obtained by way of contract or consent.
- The right to object: we accept objections from individuals to the way their data is processed and will stop processing data unless that data has been processed on the grounds of legitimate interests or in the performance of a task in the interest/exercise of official authority.
- Rights related to automated decision-making including profiling: we do not process data according to decisions made with no human involvement.

Data protection by design and default

The BISC has committed to ensure that data protection principles are embedded in all processes and activities by default.
Internal data sharing

Personal data is shared between BISC departments only as necessary to complete specific tasks and is retained only as long as is necessary to complete that task. Individuals are notified of how their data is used by different departments through the relevant privacy notice or at the point at which the data is collected.

Transfers of personal data outside the UK

The BISC shares personal data with Queen’s main campus and other third parties as specified in its privacy statements. Where data is shared with companies outside the UK, or where data is processed on behalf of the BISC by companies outside of the UK, the BISC as data controller ensures that the personal data it shares is processed in accordance with the same data protection principles as defined in this policy/by UK data protection law.

Direct marketing

Where the BISC undertakes direct marketing, it does so in accordance with the DPA Privacy and Electronic Communications (EC Directive) Regulations 2003.

Data protection training

All BISC employees carry out training on data protection at the start of their role at the BISC, and annually thereafter.

Data breaches

Anyone identifying a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data should report it immediately or as soon as it is known to the DPO, who will then apply the data breach process.
## Responsibilities:

<table>
<thead>
<tr>
<th>Contact Officer(s)</th>
<th>Responsible for:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sarah Butler</td>
<td>Data Protection Policy</td>
</tr>
<tr>
<td>Data Protection Officer</td>
<td></td>
</tr>
</tbody>
</table>

## Date for Next Review:

1 June 2024

## Related Documents:

- Implementing the BISC Data Protection Policy – guideline
- Storing and sharing personal data securely - guideline
- Collecting and using data for direct marketing – guideline
- Managing a data breach - procedure
- Responding to subject access requests - procedure

## Superseded by:

N/A.