ST BRENDAN'S
SIXTH FORM COLLEGE

[Agenda 231115 § 11.15]

# Data Protection Policy

| | |
|---|---|
| Revision number | 2023-10 |
| Approved by Audit Committee | |
| Review Date | October 2024 |

## 1.0 Policy statement

St Brendan's Sixth Form College will, as required by law, comply with the General Data Protection Regulations, 2016 ("GDPR") and the Data Protection Act 2018.

## 2.0 Scope of GDPR

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) 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;

e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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.

## 3.0 Defining 'personal data'.

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. e.g. name, identification number, location data, photo, or online identifier.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

<u>Sensitive personal data</u>

The GDPR refers to sensitive personal data as "special categories of personal data" - genetic data, and biometric data where processed can uniquely identify an individual.

## 4.0 Legitimate purposes

GDPR sets out the following as legitimate reasons for processing personal data.

a. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c. processing is necessary for compliance with a legal obligation to which the controller is subject;
d. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

## 5.0 Privacy notices

Privacy notices will describe clearly the data held for each type of data subject, the legitimate reason for its processing, how long the data will be held, and how the data subjects can request access to that data. They will also describe any agency or third party to whom data will be shared or from whom data will be received for processing. Notices will set out the rights of data subjects:

- to be informed
- of access
- to rectification
- to erasure
- to restrict processing
- to data portability
- to object
- with respect to automated decision-making and profiling.

## 6.0 Data Asset Register

The College will maintain a Data Asset Register which is a record of all the datasets containing personal data that is operated by it. The Register will include details of:

- what the dataset is
- what format it is stored in
- where it is stored
- who is responsible for it
- the legitimate purpose for processing it
- whether consent is required
- whether there is a third party processor and if there is a processing agreement in place
- how the data is collected
- how the data will be maintained
- how the data will be deleted
- when the data will be deleted

The Data Protection Officer will be responsible for maintaining the Register which will be stored on the College's SharePoint site under Governance.

Datasets containing personal data may only be constructed with the prior approval of the Data Protection Officer.

**7.0 Document Retention Schedule**
The College will maintain a Document Retention Schedule which will set out the time periods documents and data will be stored. The Schedule will be reviewed at least once every two years by the Principal and their management team.

**8.0 Staff training**
Staff will be trained in their responsibilities under GDPR / Data Protection on their induction and through regular refresher sessions and communications.

**9.0 Student training**
At induction students will be made aware of the importance of protecting their and other data subjects' personal data.

**10.0 Ways of working**
The College will operate in ways to protect its data subjects' data including through the following practices.

*Paper records*
Paper records containing personal data must be current (i.e. within retention policy timeframes) and stored under lock and key. A clear desk policy will apply to avoid the accidental access to sensitive data. Unnecessary paper records containing personal data must be disposed of immediately either through shredding or through commercial, controlled document disposal.

*Staffshare*
Drive must be cleared of all personal data (that is data that can directly or indirectly identify individuals) unless it is recorded on the Dataset Register (held by the Head of MIS and Exams) and there is a current, valid processing need. The Staffshare Drive can continue to be used for information sharing within restricted, designated user groups.

*H: Drives*
H: Drives must be cleared of all personal data (that is data that can directly or indirectly identify individuals) unless it is recorded on the Dataset Register (held by the Head of MIS and Exams) and there is a current, valid processing need.

Memory sticks incorporating hardware encryption should be used as standard. Memory sticks without encryption must not be used for any College related data. Encrypted memory sticks will be provided by IT where there is a business need.

All College laptops used by staff must be encrypted.

No College related data should be stored on any personal computer or electronic device.

Internal email will not be used for transmitting personal data in documents. Links to OneDrive should be used instead. Where personal information needs to be sent via email and the use of file sharing is not appropriate abbreviations and or reference numbers rather than names should be used.

External email containing personal data must be password protected as a minimum, with the password

being sent separately, and there must be a legitimate reason for processing the data. Secure systems should be used for sharing personal data with the appropriate authorities rather than via email.

The College will operate CCTV for the protection of persons and property on site. All recordings will be deleted from servers, including back-up servers, after 30 days other than sections of recordings held for matters of police interest, disciplinary proceedings or insurance purposes, which will removed after the conclusion of such matters.

**11.0 Breach procedures**
In the event of a breach of GDPR the procedures can be found at
https://sharepoint.stbrn.ac.uk/sites/staff/_layouts/15/WopiFrame.aspx?sourcedoc=/sites/staff/Strategy%20Policies%20and%20Procedures/Procedures/Data%20Breach%20Procedure.docx&action=default

**12.0 Privacy impact assessments**
Changes to existing systems or new systems which involve or potentially involve processing personal data will be assessed prior to implementation to test the impact on the College's compliance with GDPR.

This should be conducted by system owner / instigator in liaison with Data Protection Officer and IT. The system should not be implemented – or staff / student data shared until this has been completed.

The Assessment Template can be provided by Data Protection Officer.

**13.0 Data Controller Details**
The College has notified the U.K. Information Commissioner that it processes personal data. The registration number of the Notification is Z6130878 and can be viewed on the ICO website : http://www.ico.org.uk. The Data Protection Officer is the Head of MIS and Exams.

**14.0 Complaints**
If you have a complaint to make about the College's treatment of your data or in respect to the responses made to your enquiries you can lodge a complaint with the Information Commissioners Office on 0303 123 1113.

Data Controller: St Brendan's Sixth Form College
Registration No: Z6130878
Registered 8 Feb 2007

Data Protection Officer: Head of MIS and Exams
Data Controller Contact: Head of MIS and Exams

Version History

| Version | Date | Changes |
|---|---|---|
| 2.0 | 01/11/2023 | Section 12.0 – link to document removed and summary of requirement and responsibility for producing DIPA added.<br><br>Role holder Job title changed of DPO / DC |