The
Sir John Brunner
Foundation

Document Control Sheet

Document Type	Policy
Document name	Data Privacy Policy
Originator	Head of Personnel
Approved by	Board of Trustees
Date approved	March 2021
Review interval	Every two years
Date of last review	March 2021
Date of next review	March 2023
Equality Act 2010 issues explored	Considered to be impact neutral

The Sir John Brunner Foundation
Northwich, Cheshire, CW9 8AF
Telephone: 01606 810020

Data Privacy Policy

1 Rationale

1.1 The Sir John Brunner Foundation needs to obtain, process and store certain information about its employees, students and other users to both operate and meet its legal and contractual obligations.

The Data Protection Act (2018), sets out the data protection principles to be adhered to when handling personal data. The Foundation is responsible for, and should be able to demonstrate compliance with, these principles:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and where necessary, kept up to date;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data are processed;
- Processed in a manner that ensures appropriate security of the personal data;
- Be processed in accordance with the data subject's rights;

1.2 The Foundation and all colleagues or any others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the Foundation has this Data Privacy Policy in place.

1.3 In addition to ensuring that the Foundation complies with the Data Protection Act (2018), all those who process or use data must ensure that they protect data which is essential to the critical functions of the Foundation from loss, contamination or destruction.

2 Extent of the Policy

2.1 The Data Privacy Policy covers all computerised and manual data processing relating to identifiable individuals.

2.2. This policy covers all Foundation users: colleagues, students, applicants and any other users.

3 Status of the Policy

3.1 This policy does not form part of the formal contract of employment, but it is a condition of employment that colleagues will abide by the rules and policies made by the Foundation from time to time. Any failure to follow the policy can therefore result in disciplinary proceedings.

3.2 Any colleague who considers that the policy has not been followed in respect of their own personal data should raise the matter with their individual Academy's Data Protection Lead in the first instance. If the matter is not resolved it should be raised as a formal grievance using the Foundation's grievance procedures.

4 Definitions

4.1 **Data Protection Act (DPA)2018**
The legal framework that controls how an individual's personal information is used by organisations, businesses or the government.

4.2 **Personal Data:**
Any information, in any form (electronic or manual files) relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

4.3 **Sensitive personal data/Special Categories of data:**
Information related to an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership; sexual orientation and health.

4.4 **The Data Controller:**
The entity who determines the purposes for which and the manner in which personal data is processed.

4.5 **Data Processing**
Any action involving personal information, including obtaining, viewing, copying, amending, deleting, extracting, storing, disclosing or destroying information.

4.6 **Data Processor:**
The entity who processes the information acting on the controller's behalf. This may sometimes be a third party/organisation who the Foundation has contracted services from.

4.7 **Consent:**
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;

4.8 **Personal Data Breach:**
A personal data breach is where there has been a breach of the security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

5 Notification of Data Held and Processed

5.1 All colleagues, students and other users are entitled to know:

- what information the Foundation holds and processes about them and why;

- how to gain access to it;
- how to keep it up to date;
- what the Foundation is doing to comply with its obligations under the DPA.

5.2 The Foundation will provide all colleagues, students and other users with access to relevant data protection information and to a standard privacy notification. This will state the types of data the Foundation holds and processes about them, and the reasons for which it is processed.

6 Responsibilities of Colleagues

6.1 In relation to their own personal information, all colleagues are responsible for:

- checking that any information that they provide to the Foundation in connection with their employment is accurate and up to date;
- informing the Foundation, through their Academy, of any changes to information, which they have provided, e.g. changes of address or contact numbers;
- checking the information that the Foundation will send out from time to time, giving details of information kept and processed about colleagues;
- informing the Foundation, through their Academy, of any errors or changes. The Foundation cannot be held responsible for any errors unless the colleague has informed the Foundation of them.

6.2 Where colleagues collect information about other individuals (e.g. about employees for the purpose of appointment, remuneration, performance management or reference writing or about students' performance, personal circumstances or ability), they must comply with the guidelines for colleagues, which are at Appendix 1.

6.3 All colleagues are responsible for informing their Academy as soon as they become aware of any data protection breach.

7 Data Security

7.1 All colleagues are responsible for ensuring that:

- Any personal data on others which they hold is kept securely.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

7.2 Colleagues should note that unauthorised disclosure or unauthorised access to personal data will usually be a disciplinary matter, and may be considered gross misconduct in some cases. **Unauthorised disclosure may also be considered a criminal offence.**

7.3 Personal information should be:

- accessible only by authorised personnel and on a strict 'need to know' basis;
- kept in a locked filing cabinet; or
- in a locked drawer; or
- if it is computerised, be protected by a password which is changed periodically (***at least once each half term***) by the logon id owner; or
- kept securely when using portable storage devices.

7.4 Colleagues should ensure their computer is "locked" if they have to move away from their computer temporarily.

7.5 The logon id owner will be held responsible for all actions and functions performed by their logon id.

7.6 Colleagues, with the relevant permissions to alter data records, should:

- be satisfied that the identity of the person making the change request is either the subject of the data, or the Parent/Guardian who holds parental responsibility for the person whom the data concerns
- Be satisfied that they have the relevant permission/access to change the data records.
- Be satisfied that all steps have been taken to ascertain the validity of the data. If this is not the case, they are responsible for following up the validity so that they are satisfied
- Be satisfied that all relevant stakeholders of the data have been notified of the change

8 CCTV

Some Foundation sites are protected by closed circuit television (CCTV).

The Foundation uses CCTV to assist in:

- protecting buildings and property from any unlawful activity
- protecting the property of colleagues, students and visitors from any unlawful activity
- ensuring that colleagues and students are safe
- maintaining discipline on site
- disciplinary incident relating to a member of colleagues or student

Recorded images are kept under secure conditions for 30 days and are then normally deleted. Exceptions include images required to support a Police investigation or insurance claim. Individuals may request these images as per section 10.2 below.

9 Student and Parent/Guardian Obligations

9.1 Students and parents and guardians must ensure that all personal data provided to the Foundation is accurate and up to date.

9.2 Any changes of data must be made by the relevant person and identification must be provided colleague. Accepted forms of identification are:

- Photographic ID card provided by an Academy
- Driving Licence or passport
- Provision of DOB, Full Address and parents' names

9.3 The colleague making the changes is responsible for ensuring that the information has been updated accurately. These should all be verified against the main student record database

10 Rights of the individual and the Foundation

Individuals have a series of rights under the DPA. These are listed below with information about how the right can be invoked.

10.1 Right to be informed

Where data is collected about an individual, they will be notified of how and why their information will be used. This will normally be via a privacy statement at the time of data collection.

10.2 Right of access

Individuals are allowed to access their personal data. Individuals have the right to obtain:

- confirmation that their data is being processed
- access to their personal data

Any person who wishes to access their personal information should contact the relevant Data Protection Lead in writing. The Foundation will provide this information within one month of receipt of the request.

A reasonable administrative fee may be charged where a request is manifestly unfounded or excessive.

10.3 Right to rectification

The Foundation will ensure information held is as accurate and complete as possible. Where information about an individual is inaccurate or incomplete, individuals are entitled to have this rectified.

Individuals should inform the relevant Data Protection Lead in writing, and the Foundation will normally respond within one month (although this may be up to two months in complex cases).

10.4 **Right to erasure (right to be forgotten)**

Where there is no compelling reason for the continued processing of personal data, individuals can request the deletion or removal of their personal data.

Individuals must inform the relevant Data Protection Lead in writing of this request. This request will not unreasonably be declined, however the DPA provides for certain circumstances when this request will be refused and these will be communicated where applicable.

10.5 **Right to restrict processing**

Individuals have the right to "block" or suppress the processing of personal data. When processing is restricted, the Foundation may store the information but not further process it.

Individuals must make their requests to the relevant Data Protection Lead in writing. Individuals will also be informed when the Foundation decides to lift a restriction on processing.

10.6 **Right to data portability**

Individuals have the right to receive the personal data concerning him or her, which he or she has provided to the Foundation, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller.

The individual may also request the information is transferred direct to another organisation where this is technically feasible.

Individuals must make such requests in writing to the relevant Data Protection Lead. A response to this request should be completed within one month (extended to two for complex cases or where a number of requests are made)

10.7 **Right to object**

Individuals have the right to object to their information being processed in relation to:

- Legitimate interests or the performance of a task in the public interest/exercise of office authority
- Direct marketing
- Scientific/historical research and statistics.

Individuals should make this request to the relevant Data Protection Lead. There are some circumstances where the Foundation will not be able to stop processing personal data, the reasons will be communicated to the individual should this be the case.

10.8 **Automated decision making and profiling**

The Foundation does not process data in a way that would constitute automated decision making. There will always be human input into decisions related to individuals.

10.9 **Right of appeal**

Where an individual has made a request, which the Data Protection Lead or the Data Protection Officer has refused. The individual may refer to the Information Commissioners Office.

10.10 **Right of refusal (Foundation)**

The Foundation has the right to refuse the individual's request for the following reasons:

- There is a legal reason not to comply
- There is a contractual reason not to comply

Any legal or contractual reason to process the individual's data must be made clear to the individual at the point of collecting the data.

11 Publication of Foundation and Academy Information

In order that the public can access details about the Foundation and its services, certain information is published on the website, this may include:

- Names and contacts of governors/Trustees
- Minutes of Corporation Meetings and its sub-committees.
- Photographs and articles relating to Academy life.

Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the Data Protection Officer.

The Foundation will comply with the demands of the Freedom of Information Act.

12 Lawful basis of processing information

12.1 The Foundation will only process personal data where a lawful basis for doing so exists. The reasons for and requirements to process data will vary according to the intended purpose.

- Consent has been provided by the individual
- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- Processing is necessary for compliance with a legal obligation
- Processing is necessary to protect the vital interests of a data subject of another person.

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of office authority vested in the controller
- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights of freedoms of the data subject.

12.2 Since all posts in the Foundation will potentially bring colleagues into contact with children, the Foundation has a duty under the Children Act and other enactments to ensure that colleagues are suitable for employment. The Foundation also has a duty of care to all colleagues and students and must therefore make sure that employees and those who use Foundation facilities do not pose a threat or danger to other users. Therefore, a DBS check will be obligatory for all successful applicants to join the Foundation staff. DBS checks will also be obligatory for all those students who undertake extensive work experience placements that will bring them into contact with children.

12.3 The Foundation will also ask for information on colleagues and students about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The Foundation will only use the information in the protection of the health and safety of the individual.

12.4 Personal data is collected at different points in time. Information notices will be provided at the appropriate times detailing how this information will be used.

13 Processing Sensitive Information/Special categories of data

13.1 Sometimes it is necessary to process information about a person's race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or biometric data, health and sexual orientation. In terms of the DPA this is known as special categories. The recording of sensitive data may be to ensure the Foundation is a safe place for everyone, or to operate other Foundation policies. Because this information is more sensitive and needs more protection, the Foundation will only process such data where there is a lawful basis to do so as well as meeting one of the specific conditions set out within the DPA.

14 Data Protection Governance arrangements

14.1 The Sir John Brunner Foundation as a corporate body is the data controller under the DPA, and the Board is therefore ultimately responsible for implementation of this policy.

14.2 The Foundation has a named Data Protection Officer, who is responsible for:

- advising and informing the Foundation about its obligations under the DPA.monitoring Foundation compliance in line with the DPA

14.3 Each individual Academy within the Foundation will appoint a Data Protection Lead who is responsible for:

- day to day operations of data protection
- being the first point of contact for the supervisory authority and the individuals whose data is being processed.

14.5 The Information and Commissioners Office is the relevant supervisory authority for the purposes of DPA.

15 Data Breaches

15.1 The Foundation is committed to ensuring data being held both electronically and in manual files are secure and accessed only by appropriate individuals who have received the relevant training.

15.2 The Foundation is legally required to notify the Information Commissioners Office of any breach where it is likely to result in a risk to the rights and freedoms of individuals (where there is likely to be any significant social or economic disadvantage). The Data Protection Officer is responsible for managing the breach and notifying the ICO were appropriate.

15.3 All colleagues are responsible for notifying the Data Protection Officer of any breach. and other relevant Heads of Department.

15.4 The Act includes onerous penalties for breaches, and there are penalties for failure to notify the ICO within 72 hours.

16 Retention of Data

16.1 Academies will keep some forms of information for longer than others.

16.2 Each Academy will retain data in accordance with their individual Record Retention Schedule.

16.3 All data on colleagues or students who have left an Academy must be stored centrally, within the relevant organisation.

17 Third Parties

It is necessary for information to be shared with third parties/organisations from time to time. This will be because they are contracted to provide services to the Foundation, or because the Foundation is legally or contractually obliged to send information about an individual/s.

Where the third party is providing a service to the Foundation, the Foundation will ensure there are appropriate guarantees in place that the data will be processed in line with DPA.