

Document Control Sheet

Document Type	Policy
Document name	Data Protection Policy
Originator	Head of Personnel
Approved by	Foundation Board
Date approved	14 December 2023
Review interval	Biennial
Date of last approval	March 2021
Date of next review	March 2025
Equality Act 2010 issues fully considered	Considered to be neutral.
Associated Policies and Procedures	

Data Privacy

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 is 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 Protection 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 Scope of the Policy

- 2.1 The Data Protection 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. For example, name, address, student ID number, date of birth, home address, email address, attendance information, photos, bank and financial information, exam and assessment results.
- 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, biometric data (where used for identification purposes), sexual orientation, a person's sex life 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 they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them;

4.8 **Personal Data Breach:**

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

4.9 **Biometric Data:**

Is personal data relating to the physical, physiological or behavioural characteristics of a person, confirming the unique identification of that person, such as facial images or fingerprints.

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 All 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 this policy.

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

7 Responsibilities of Students and Parents/Guardians

- 7.1 Students, parents and guardians must ensure that all personal data provided to the Foundation through their Academy is accurate and up to date.

- 7.2 Any changes of data must be made by the relevant person and identification must be provided to the Academy. Accepted forms of identification are:

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

- 7.3 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

8 Data Security

- 8.1 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.

- 8.2 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.**

- 8.3 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 term or half termly for those with higher access**) by the logon id owner or as required by the Academy's IT security procedures; or
- kept securely when using portable storage devices.

- 8.4 Colleagues should ensure their computer is “locked” if they have to move away from their computer temporarily.
- 8.5 The logon id owner will be held responsible for all actions and functions performed by their logon id.
- 8.6 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

9 Recording Meetings

- 9.1 In the normal course of Foundation business, meetings will take place. For some meetings it will be necessary or useful to take a note of the nature of the discussion and/or the agreed actions arising from the meeting.
- 9.2 Where notes of a meeting are taken, these will not necessarily be verbatim but will be an accurate summary of the discussion and will capture all the key points made.
- 9.3 Any electronic recordings of meetings that contain a significant amount of personal data must only be made by using Foundation licensed tools such as Microsoft Teams. Such recordings must be stored securely within the Foundation licensed system. When recording a meeting the participant(s) must be informed that a recording is being made and understand:
- What the recording is for and how it will be used
 - Who will have access to it
 - How long it will be kept for
- 9.4 Where recordings are made of sensitive meetings or where a meeting participant withholds consent for the recording to be shared, access to the recording may be only available for the generation of an accurate transcript by a scribe. In such cases a written summary of the meeting should be made available to all participants.

10 Rights of the Individual and the Foundation

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

10.1.1 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.

10.1.2 Right of access (see section 20)

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.

10.1.3 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).

10.1.4 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.

10.1.5 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.

10.1.6 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).

10.1.7 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.

10.1.8 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.

10.1.9 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.

10.1.10 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

- 11.1 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 contact details of Governors/Trustees
 - Minutes of Corporation Meetings and its sub-committees.
 - Photographs and articles relating to Academy life.
- 11.2 Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the Data Protection Officer.
- 11.3 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.
- 14.4 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 is 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 Lead is responsible for managing the breach and notifying the ICO where appropriate. Data Protection Leads should also notify the Foundation Data Lead.
- 15.3 All colleagues are responsible for notifying the Data Protection Lead of any breach using the relevant reporting mechanism
- 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 the Foundation's Record Retention Schedule.
- 16.3 All data on colleagues or students who have left an Academy must be stored centrally, within the relevant department.

17 Third Parties

- 17.1 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.
- 17.2 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.

Closed Circuit Television (CCTV)

18 CCTV

- 18.1 Some Foundation sites are protected by CCTV.

- 18.2 The Foundation seeks to operate its CCTV systems in a manner that is consistent with respect for the individual's privacy and our safeguarding obligations.
- 18.3 Cameras are used to monitor activities within Foundation buildings, sites, car parks and other areas to:
- protect Foundation buildings and property from any unlawful activity
 - protect the property of colleagues, students and visitors from any unlawful activity
 - ensure that colleagues and students are safe
 - be used if required for any disciplinary incidents relating to colleagues or students
- 18.4 Each Academy will nominate a senior manager to be responsible for the overall management and operation of the CCTV system, including activities relating to installations, recording, reviewing, monitoring and ensuring compliance with this policy.
- 18.5 The CCTV will only be operated and accessed by Authorised Post holders in Academies with explicit authority.
- 18.6 CCTV systems must only be accessed:
- by Authorised Post holders or an individual to whom they have delegated authority
 - in accordance with this Policy
 - for the reasons set out in Section 18.3
 - with respect for the privacy of individuals
- 18.7 Recorded images are kept under secure conditions for 28 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 20 below.
- 18.8 CCTV images may be released where disclosure is necessary for the purposes for which the images were recorded or where permitted/required by law.
- 18.9 The Foundation retains the right to refuse any request unless there is an overriding legal obligation.
- 18.10 All requests for the disclosure of images should be made to the Academy Data Protection Lead. The Data Protection Lead will put the request to the relevant

authorised post holder with whom the decision to disclose the images or not will rest.

18.11 A record of all requests for disclosure under this policy will be retained, together with the reasons for agreeing to or refusing the request. Where disclosure is approved, the following will also be recorded:

- The reason for disclosure
- The authorised post holder making the disclosure
- The identity of the individual or organisation making the request
- The date and time the images were recorded
- The location of the images and the relevant camera
- Details of information being released
- The date the images were released
- Any relevant crime incident or insurance policy number

18.12 Third party requests for CCTV images will only be considered from the following:

- The police or other law enforcement agencies when their request is in pursuit of a crime
- Prosecution agencies
- Relevant legal representatives
- Relevant insurance companies

Protection of Biometric Data

19 Automated Biometric Recognition Systems

- 19.1 An automated biometric recognition system is a system which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify the individual. In some academies an automated biometric recognition system is used as the cashless payment system.
- 19.2 Where an Academy uses student and/or staff biometric data as part of an automated biometric recognition system the Academy will comply with the requirements of the Protection of Freedoms Act 2012.
- 19.3 In the case of students, the Academy will notify each parent/guardian of their intention to process the student's biometric information. A student's biometric information will not be processed unless at least one parent of the child consents and no parent has withdrawn their consent or otherwise objected to the information being processed. A student's objection or refusal will override any parental consent to the processing.
- 19.4 If consent is withdrawn any biometric data that has already been captured will be deleted.
- 19.5 Notification sent to parents/guardians about the use of biometric data will include information regarding the following:
- Details about the type of biometric information to be taken
 - How the data will be used
 - The parent's and the pupil's right to refuse or withdraw their consent
 - The Academy duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed
- 19.6 Where an individual objects to taking part in the Academy's biometric system(s), reasonable alternative arrangements will be provided that allow the individual to access the relevant service, e.g. where a biometric system uses student's fingerprints to pay for meals, the student will be able to use cash for the transaction.
- 19.7 Where colleagues use the biometric system consent will be obtained before they use the system.

Data Subject Access Requests

20 Data Subject Access Requests

- 20.1 All data subjects have rights of access to their personal data. A data subject access request (DSAR) is when an individual makes a request for a copy of the personal data an organisation holds on them or details of what data is held and its source.
- 20.2 Whilst ideally DSARs will be submitted to the Data Protection Lead requests can be made to any individual in the Academy. They can be made in writing, by email, or verbally. If a colleague receives a request for information, they should inform their Academy's Data Protection Lead as soon as possible.
- 20.3 The Academy will supply data that is held as electronic records and paper records that are part of a filing system, for which it is the data controller. In most cases the Academy will not supply data that is stored on third party systems for which it is not the controller. The Academy may also be unable to supply data contained within an email encryption software, which is not a filing system, and which may have a different retention policy to the Foundation. It is recommended that any relevant information shared with the Academy should be moved from these encryption systems and retained in the relevant file, in accordance with the Foundation's Record Retention Schedule.
- 20.4 In most cases a DSAR will be responded to free of charge, however the Academy may charge a reasonable administrative fee for additional copies requested by the data subject, or if requests are manifestly unfounded or excessive.
- 20.5 There are circumstances where information can be withheld from a DSAR. These are specific exemptions and requests will be considered by the Academy on a case by case basis. In exceptional circumstances, the Academy may refuse to respond to a request, for example if the request is deemed to be manifestly unfounded/excessive, if the request involves disclosing information relating to a third party which cannot be redacted or the information contains legal privilege. If the Academy has to refuse a request, this will be confirmed in writing to the data subject.
- 20.6 When a DSAR is received, the Academy will:
- acknowledge the receipt in writing, usually within 5 working days.
 - satisfy itself of the identity of the data subject as appropriate.
 - contact the data subject to ask them to specify the information or processing activities their request relates to if necessary.
 - take all reasonable and proportionate steps to identify and disclose the information relating to the request.
 - redact any references to third parties within the data where relevant.
 - respond to the request in writing and provide the information either in hard copies or electronic format, according to the request.

- respond to the request within one calendar month, unless the request is complex – see 20.8. This period starts counting from the latest of:
 - The date the request is made,
 - the date the Academy has received proof of identity from the data subject
 - Payment of any fee

20.7 When responding to a DSAR the Academy will provide the data subject with:

- The purposes of the processing
- The categories of personal data involved
- The recipients the personal data has been or will be disclosed to
- The length of time the data will be retained (or if this is not possible, the criteria for determining the retention period)
- The existence of the data subject's right to request that the Academy rectify or erase the personal data or restrict processing or to object to processing
- The data subject's right to lodge a complaint with the Information Commissioner's Office
- Where the personal data has not been collected directly from the data subject, any available information about its source
- The existence of any automated decision making, including profiling and meaningful information about the logic involved as well as the significance and the envisaged consequences for the data subject of such processing
- The safeguards we have provided where personal data has or will be transferred to a third country or international organisation.

20.8 The period for response may be extended by a further two calendar months for complex requests. If the Academy decides it is necessary to extend the time limit they will let the data subject know within one month of receiving the request and will explain why.

20.9 A data subject is generally only entitled to access their own personal data, and not to information relating to other people. However, an individual may prefer a third party (e.g. a relative, parent or solicitor) to make a SAR on their behalf. Before responding to a third party request the Academy must be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide the Academy with evidence of this.

In most cases parents/guardians do not have automatic rights to the personal data of their child. In the case of requests for data from a parent the Academy will consider the particular circumstances and consider whether the student is mature enough to understand their rights. If it is deemed that the student can understand their rights, the response for data should be directed to the student rather than the parent. As a general rule, consent must be obtained from students who are 12 years and older before the data is released.