The
Sir John Brunner
Foundation

DATA PROTECTION POLICY

APRIL 2025

Excellence | Belonging | Partnership

The
Sir John Brunner
Foundation

Document Control Sheet

Document Type	Policy
Document name	Data Protection Policy
Originator	Chief Financial & Operations Officer
Approved by	Foundation Board
Date approved	02 April 2025
Review interval	Biennial
Date of last approval	December 2023
Date of next review	March 2027
Equality Act 2010 issues fully considered	Considered to be neutral.
Associated Policies and Procedures	SJBF GDPR Framework Records Management Policy Information Security Policy

The Sir John Brunner Foundation
Northwich, Cheshire, CW9 8AF Tel: 01606 664900

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; and
- 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.

1.4 This Policy forms part of the Sir John Brunner Foundation GDPR Framework.

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, governance, applicants and any other users.

2.3 For the purposes of this policy, where there is reference to an **'academy'**, this refers to any academies within the Sir John Brunner Foundation and the central teams within the Foundation.

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.

UK GDPR:
The UK GDPR is the UK's implementation of the EU General Data Protection Regulation (GDPR). The UK GDPR sits alongside an amended version of the DPA 2018 and the key principles, rights and obligations remain the same.

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. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the GDPR personal information also includes an identifier such as a name, an identification number, location data or an online 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, 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 **Automated Decision Making (ADM):**
When a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits automated decision-making (unless certain conditions are met) but not automated processing.

4.10 **Automated Processing:**
Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of automated processing.

4.11 **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 Key Principles

5.1 There are 6 enforceable principles contained in Article 5 of the General Data Protection Regulations, which the Foundation must adhere to when processing personal data.

- Principle 1 – Personal data shall be processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency)

- Principle 2 – Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation)

- Principle 3 – Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (data minimisation)

- Principle 4 – Personal data shall be accurate and where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay. (accuracy)

- Principle 5 - Personal data shall be 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)

- Principle 6 (the Security Principle) - Personal data shall be processed in a manner that ensures appropriate security of the data, including protection

against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data, using appropriate technical or organisational measures. (integrity and confidentiality)

5.2 There is a 7th Principle - the Accountability Principle which requires organisations to take responsibility for what they do with personal data and how they comply with the other principles. At the Foundation, the responsibility for adherence to the principles lies with all staff.

5.3 The organisation must have appropriate measures and records in place to be able to demonstrate their compliance.

5.4 In addition to adherence to the principles, there are transfer limitations relating to the transfer of personal data to a country outside the EEA. Should an occasion arise requiring such a transfer, members of staff should contact the Data Protection Officer for assistance.

5.5 The Foundation has overall commitment to compliance with the above principles.

5.6 Alongside actions relating to specific obligations with which the legislation obliges the Foundation to comply, and which are included below in relevant sections of this Policy, the Foundation will:

(a) Produce an information asset register that contains details of the records it holds.

(b) Inform individuals why the information is being collected at the point it is collected by way of privacy notices.

(c) Inform individuals when their information is shared, and why and with whom it will be shared.

(d) Check the quality and the accuracy of the information it holds.

(e) Ensure that information is not retained for longer than is necessary.

(f) Ensure that when obsolete, information is destroyed and it is done so appropriately and securely.

(g) Create and maintain a Record Management Policy setting out record retention and disposal dates for common data sets and other information.

(h) Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.

(i) Share information with others only when it is fair and lawful to do so and satisfies the lawful basis for processing that information (lawful bases are set out in section 13).

(j) Share personal data with other organisations for the purpose of crime prevention and/or detection, or for the purpose of legal proceedings, provided that the disclosure falls within an exemption to the non-disclosure provisions contained within the Data Protection Act 1998 or any subsequent legislation.

(k) Disclose personal data where required to do so by law for example, following receipt of a court order.

(l) Set out procedures to ensure compliance with the duty to respond to an individual's rights to:

- request access to personal information, known as Subject Access Requests.
- be informed about the way their data is used.
- have inaccurate personal data rectified.
- have their personal data erased.
- restrict the processing of their personal data.
- object to the processing of their personal data.

(m) Ensure the Foundation's staff are appropriately and regularly trained and aware of and understand the Foundation's policies and procedures.

(n) Create and maintain a data breach notification to record data breaches and also circumstances where a breach was narrowly avoided.

6 Notification of Data Held and Processed

6.1 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; and
- what the Foundation is doing to comply with its obligations under the DPA.

6.2 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.

7 Responsibilities of All Colleagues

7.1 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; and
- 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.

7.2 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.

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

8 Responsibilities of Students and Parents/Guardians

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

8.2 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'/carers names

8.3 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

9 Data Security

9.1 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.

9.2 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.**

9.3 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 by the logon id owner or as required by the Academy's IT security procedures; or
- kept securely when using portable storage devices.

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

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

9.6 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.

10 Recording Meetings

10.1 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.

10.2 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.

10.3 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

10.4 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.

11 Rights of the Individual and the Foundation

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

11.1.1 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. Individuals have the right to be notified of a data breach which is likely to result in high risk to their rights and obligations.

11.1.2 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.

11.1.3 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).

11.1.4 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.

11.1.5 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.

11.1.6 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).

11.1.7 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 and the reasons will be communicated to the individual should this be the case.

11.1.8 Automated decision making and profiling

The Foundation does not process data in a way that would constitute automated decision making. Whilst the Foundation may utilise profiling in the course of its business, there will always be human input into decisions related to individuals.

11.1.9 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.

11.1.10 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.

12 Publication of Foundation and Academy Information

12.1 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.

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

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

13 Lawful basis of processing information

13.1 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 and rights of freedoms of the data subject, in particular where the data subject is a child.

13.2 Where the lawful basis for processing is consent this must be clearly evidenced by a very clear and specific statement. Such consent requires a positive opt-in and so pre-ticked boxes or any other method of default consent will not be sufficient. If consent is given in a document which deals with other matters, the consent must be kept separate from those other matters. The data subject shall have the right to withdraw his or her consent at any time and withdrawal must be promptly honoured. Prior to giving consent, the data subject shall be notified of the right of withdrawal.

13.3 Unless the Foundation can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data. In such circumstances the Foundation will obtain evidence of and record consent so that it can demonstrate compliance with the GDPR.

13.4 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.

13.5 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.

13.6 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.

14 Processing Sensitive Information/Special categories of data

14.1 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. As 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.

14.2 The Foundation's privacy notices set out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

15 Data Protection Governance arrangements

15.1 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.

15.2 The Foundation has a named **Data Protection Officer** Kathryn McBurnie (CFOO). The DPO cannot hold a position that requires them to determine the purpose and means of processing personal data. For this reason, the Foundation uses a Trust Data Protection Lead to develop the Data Protection Framework for the Foundation. The DPO can be contacted at kmcburnie@sjbf.org.uk or 01606 664902. The DPO is responsible for:

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

15.3 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.
- ensuring the academy follows the Record Management Policy, including the Foundation Document Retention Schedule.

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

16 Data Protection Impact Assessments (DPIA)

16.1 The Foundation will carry out a DPIA when processing is likely to result in high risk to the data protection rights and freedoms of individuals.

16.2 The GDPR does not define high risk, but guidance highlights a number of factors that are likely to trigger the need for a DPIA, which include:

- The use of new technologies
- Processing on a large scale
- Systematic monitoring
- Processing of special categories of data

16.3 The purpose of the DPIA is to assess:

- Whether the processing is necessary and proportionate in relation to its purpose.
- The risks to individuals, including both the likelihood and the severity of any impact on them.
- What measures can be put in place to address those risks and protect personal information.

16.4 Staff should refer to the DPIA template that is available on the GDPRiS platform or from the Academy Data Protection Lead. When carrying out a DPIA staff should seek the advice of the Academy Data Protection Lead and DPO for support and guidance and once complete, refer the finalised document to the DPO for sign off.

17 Records of Processing Activity

17.1 The Foundation in accordance with its duty as a Data Controller and Data Processor will keep detailed records of data processing activities (ROPA) and the records shall contain:

- The name and contact details of the Foundation and its Academies and, if applicable, of any joint controllers;
- The name and contact details of the DPO;
- The name and details of individuals or roles that carry out the processing;
- The purposes of the processing;
- A description of the categories of individuals i.e. the different types of people whose personal data is processed;
- Categories of personal data processed;
- Categories of receipts of personal data;

- Details of any transfers to third countries, including documentation of the transfer mechanism safeguards in place;
- Retention schedules; and
- A description of technical and organisational security measures.

18 Security of personal data

18.1 The security principle requires that appropriate security is put in place to prevent personal data being accidentally or deliberately compromised. In order to comply with this principle the Foundation will:

- Ensure that all individuals involved in processing data understand the requirements of confidentiality, integrity and availability for the personal data being processed.
- Undertake an analysis of the risks presented by its processing, and use this to assess the appropriate level of security it needs to put in place to keep paper and electronic personal data secure and ensure that appropriate security measures are enforced.
- Ensure that only authorised individuals have access to personal data.
- Put in place appropriate physical and organisational security measures, as well as technical measures, and regularly review the physical security of the Foundation buildings and storage systems.
- Require staff to ensure that no personal data will be left unattended in any vehicles and that if it is necessary to take personal data from Foundation premises, for example to complete work from home, the data is suitably secured.
- Review the Information Security Policy regularly and takes steps to make sure the policy is implemented.
- Use encryption and/or pseudonymisation where it is appropriate to do so.
- Ensure that all portable electronic devices containing personal data are password protected.
- Refer to any relevant guidance and seek advice where necessary if processing personal data utilising a cloud based solution.
- Make sure that it can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.
- Ensure that any data processor it uses also implements appropriate technical and organisational measures.

19 Data Breaches

19.1 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.

19.2 What constitutes a data breach? Under the UK GDPR, a personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data – whether due to accidental or deliberate causes. It is a security incident that affects the confidentiality, integrity, or availability of personal data. Some examples of possible data breaches include: • an unauthorised third party accessing personal data; • an organisation sending personal data to an incorrect recipient; • computing devices containing personal data being lost or stolen; • the alteration of personal data without appropriate permission; and • the loss of availability of personal data.

19.3 A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored
- Unauthorised access to or use of personal information either by a member of staff or third party
- Loss of data resulting from an equipment or systems (including hardware or software) failure
- Human error, such as accidental deletion or alteration of data
- Unforeseen circumstances, such as a fire or flood
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- Blagging offences where information is obtained by deceiving the organisation which holds it
- Sending personal data to an incorrect recipient
- The alteration of personal data without appropriate permission

19.4 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). Any data breaches (or near misses) should be reported on the GDPRiS platform. The Data Protection Lead is responsible for managing the breach and notifying the ICO were appropriate. Data Protection Leads should also notify the Foundation Data Lead.

19.5 All colleagues are responsible for notifying the Data Protection Lead of any breach using the relevant reporting mechanism.

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

20 Retention of Data

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

20.2 Each Academy will retain data in accordance with the Foundation's Record Management Policy, to ensure personal data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time.

20.3 Staff will take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required in accordance with the Policy. This includes requiring third parties to delete such data where applicable.

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

21 Third Parties

21.1 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.

21.2 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.

22 Photographs, electronic images and Closed Circuit Television (CCTV)

22.1 Some Foundation sites are protected by CCTV. The Foundation adheres to the ICO's Code of Practice for the use of CCTV.

22.2 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.

22.3 There is no requirement to ask individuals' permission to use CCTV, but the Foundation has to make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

22.4 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

22.5 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.

The CCTV will only be operated and accessed by Authorised Post Holders in Academies with explicit authority.

22.6 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

22.7 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.

22.8 CCTV images may be released where disclosure is necessary for the purposes for which the images were recorded or where permitted/required by law.

22.9 The Foundation retains the right to refuse any request unless there is an overriding legal obligation.

22.10 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.

22.11 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

22.12 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

Photographs and Videos

22.13 As part of the Foundation's activities, we or a 3rd party (e.g. school photographers) may want to take photographs and record images of individuals

within the school. The relevant academy will obtain *written* consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

22.14 Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

22.15 When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

23 Biometric Data: Automated Biometric Recognition Systems

23.1 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.

23.2 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.

23.3 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.

23.4 If consent is withdrawn any biometric data that has already been captured will be deleted.

23.5 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

23.6 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.

23.7 Where colleagues use the biometric system consent will be obtained before they use the system.

24 Access to Personal Data and Data Subject Access Requests

24.1 There are 2 distinct rights of access to information held by the Foundation about pupils, parents/carers and staff:

- Pupils and parents or those with Parental Responsibility have a right to make a request under the GDPR to access the personal information held about them.
- Pupils and parents or those with Parental Responsibility have a right to access the educational records. The right of those entitled to have access to curricular and educational records is defined within the Education (Pupil Information) (England) Regulations 2005.

24.2 All data subjects have rights of access to their personal data. Article 15 of the GDPR gives individuals the right to access personal data relating to them, processed by a data controller. The right can be exercised by a person with Parental Responsibility on behalf of their child dependent on the age and the understanding of the child. 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.

24.3 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, via social networks or verbally. If a colleague receives a request for information, they should inform their Academy's Data Protection Lead as soon as possible and record the request on the GDPRiS platform.

24.4 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.

24.5 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.

24.6 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.

24.7 The identity of the requestor must be established before the disclosure of any information is made. Proof of a relationship with a child (where applicable and if not known) must also be established as this will verify whether the individual making the request can lawfully exercise that right on behalf of the child.

24.8 The process for responding to a DSAR is contained within the Foundation Subject Access Request Procedure Note.

24.9 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.

24.10 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.

24.11 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 13 years and older before the data is released.

25 Complaints

25.1 Subject to paragraphs 25.2 and 25.3, complaints relating to the Foundation's compliance with the GDPR will be dealt with in accordance with the Foundation's Complaints Policy.

25.2 Complaints relating to access to personal information or access to education records should be made to our DPO who will decide whether it is appropriate for the complaint to be dealt with through the Foundation's complaints procedure. Complaints which are not appropriate to be dealt with through the Foundation's complaints procedure can be referred to the Information Commissioner. Details of how to make a complaint to the ICO will be provided with the response letter.

25.3 Complaints relating to information handling may be referred to the Information Commissioner's Office (the statutory regulator). Contact details can be found on their website at www.ico.org.uk or telephone 0303 123 1113.