
# Data Protection Policy

**Headteacher**: Stephen Mitchell

**Chair of Governors**: Alexandra Woolmore

**Ratified**: March 2024

**Review:** March 2026

## 1. Introduction and Scope

1.1 The General Data Protection Regulation (GDPR), Data Protection Act 2018, and the Privacy and Electronic Communication Regulations are the laws governing the processing of personal data in the United Kingdom. They apply to anyone that uses personal data for non-domestic uses.

1.2 This policy sets out how King's Cross Academy processes personal data and complies with the legislation referred to in section 1.1 and covers all processing of personal data whether in electronic or paper formats.

1.3 King's Cross Academy is a Data Controller registered with the Information Commissioner's Office (ICO) ZA099429 and must comply with the regulations in the processing of personal data, including the way in which the data is obtained, stored, used, disclosed and destroyed. The Academy must be able to demonstrate compliance. Failure to comply exposes the Academy to civil claims and/or enforcement action from the ICO that may include financial penalties.

1.4 Staff, when processing personal data for Academy business, are acting on behalf of the Data Controller, and for avoidance of doubt, when this policy refers to actions the Academy shall take, it also means the staff involved with the processing of relevant personal data.

1.5 This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the Academy. Any failures to follow this policy may result in disciplinary proceedings.

## 2. Personal Data

2.1 Personal data only includes information relating to natural persons who can be identified or who are identifiable, directly from the information in question, or who can be indirectly identified from that information in combination with other information (for example: name, address, date of birth, National Insurance number, bank account details etc.).

2.2 Personal data may also include special categories of personal data. This is information about racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or condition, sexual life, biometric data (e.g. finger prints). Criminal offence data includes information about allegations and status as a victim/survivor of a crime, as well as convictions and sentences.

2.3 King's Cross Academy will only collect and process personal, special category, and criminal offence data for specific purposes where required or permitted by law, or where consent is required, the necessary consents have been received.

2.4 The Academy is required to adhere to the six Data Protection Principles specified in article 5.1 of the GDPR. The Academy is also required to maintain records that demonstrate this compliance by article 5.2 of the GDPR. This is achieved by this policy document, maintaining a record of processing activities in an Information Asset Register, and any further policies that are specific to those processing activities.

2.5 This policy deals with the Data Protection Principles in sections 4 through 9.

## 3. Data Protection Officer

3.1 The Academy is required by the legislation to appoint a Data Protection Officer (DPO). The Data Protection Officer is Andrew Maughan, Borough Solicitor for the London Borough of Camden. He can be contacted at Academysdpo@camden.gov.uk or 0207 974 4365. The Data Protection Officer is supported by the Data Protection Advice Team that monitor these contact details and carry out business-as-usual tasks on his behalf.

3.2 The role of the Data Protection Officer helps the Academy to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

**3.3** Should data subjects, e.g. pupils, parents, or staff, have concerns or enquiries regarding Data Protection, they should in the first instance discuss these with the Academy's leadership. But if this is not possible or not practical in the circumstances, they may contact the DPO directly.

## 4. Fair, lawful, and transparent.

**4.1** The Academy will handle Personal Data fairly, lawfully and transparently:

4.1.1 The Academy will only process Personal Data in ways which would reasonably be expected of an Academy and will be honest and transparent about the reasons for any processing. Should there be any processing required which may be unexpected or unusual, Academy leadership in conjunction with the DPO will take steps to inform the subjects as far as reasonably possible under the circumstances. This may take the form of an extra Privacy Notice. (See Section 4.3 (Privacy Notices))

4.1.2 If there may be any adverse effects on data subjects due to processing the Academy will consider these and be able to justify any such processing. See section 11 – Data Protection Impact Assessments.

4.2 The Academy commits to handle personal data lawfully by assessing the lawful basis for all significant processing activity. This will be maintained in the Information Asset Register, and where necessary, recording in a DPIA.

4.3 The Academy is committed to transparency and upholding the right of the data subject to be informed of how their data is being processed. This is normally done through providing a copy of, or a link to, the Academy's Privacy Notice on our website. Additional Privacy Information may be communicated with data subjects as required.

4.3.1 This Privacy Notice or additional information will be provided at the time the information is collected. Should the information be obtained from a third party, such as the Local Authority or Department of Education, the Academy will normally provide this information within 30 calendar days.

## 5. Purposes of processing

5.1 The Academy shall process data only for the purposes it was originally collected, or compatible purposes. The purposes will be communicated with the data subject in a Privacy Notice as per section 4.

5.2 Should a need arise to process data in an additional or different way to the purposes originally specified, the Academy's leadership shall consult the DPO regarding a Data Protection Impact Assessment. The new purposes must be found to be lawful and fair, and then communicated transparently as per section 4.

## 6. Data Minimisation

6.1 The Academy will not collect more data than it requires. For significant processing activities, the Information Asset Owners listed in the Information Asset Register will be responsible for ensuring that only the minimum information required for the specified purpose is held, and no more. Often this will involve reviewing forms that are used to collect data, and ensure that there are not fields collecting information that is no longer used.

6.2 For any other processing carried out on behalf of the Academy, the staff carrying out the processing will be responsible for compliance with this principle. In summary, staff should assess the need to collect personal data before doing so, and only collect personal data when necessary, and then only the minimum data required.

## 7. Data Accuracy

**7.1** For significant processing activities, the Information Asset Owners listed in the Information Asset Register shall be responsible for ensuring accuracy of data. This will involve an assessment of the risks associated with the data being or becoming inaccurate and implementing an appropriate procedure for ensuring the data obtained is accurate and is kept accurate.

7.2 Individual staff remain responsible for keeping and maintaining their own accurate records for any other processing undertaken.

## 8. Retention and Destruction

**8.1** Personal data shall be kept only for as long as it is required for the purpose it was collected for and no longer.

**8.2** The Academy follows the Academy's retention guidance which specifies how long information is kept for.

8.3 Each entry in the Information Asset Register shall have a corresponding entry in the Retention and Destruction Policy.

8.4 The Information Asset Owners are responsible for ensuring deletion/destruction is carried out in accordance with the Retention and Destruction Policy, and also for keeping the necessary records to show that data have been appropriately destroyed.

8.5 Other records (those not included in the Asset Register) may also be included in the Retention and Destruction Policy to assist with managing files. Staff will seek advice if uncertain about how long they should be keeping a record.

## 9. Information Security

**9.1** For significant processing activities, the Information Asset Owners listed in the IAR shall be responsible for carrying out a risk assessment and ensuring security measures in place adequately reflect the risks associated with that processing. This is in addition to any basic requirements set out below.

9.1.1 Staff must store data securely at all times and should never store data, even temporarily, where it may be at risk (e.g. staff must not take data to a pub or restaurant on the way home, or leave it in the back of a car overnight or when at the supermarket).

9.1.2 Paper based information should only be carried outside the organisation if absolutely necessary and only with the explicit approval of the Head Teacher or authorised deputy.

9.1.3 This information should not be read or displayed on public transport, or in public spaces due to the risk of unauthorised disclosure.

9.1.4 Where it is absolutely necessary to keep confidential information at home (for example key emergency contact details or business continuity plans) as sanctioned by a manager with the necessary authority, these documents must be kept securely under lock and key. This means that such information should be stored in a private lockable cupboard or similarly secure space, and should be kept out of sight (e.g. not left on tables or in hallways where it would be visibly obvious to unauthorised persons, such as housemates, or intruders).

9.1.5 Paper based information should also be stored separately from high value items such as laptops wherever possible, and should not be kept together in a laptop bag.

9.1.6 Staff must ensure they know who to contact for security advice and guidance, including when working remotely, and how to contact them.

## 10. Automated processing and decision making

The Academy does not carry out any automated processing or decision making using personal data.

### 10.1 Individual Rights

### 10.2 Subject Access

10.2.1 Individuals (“Data Subjects”) have the right to access their personal data. The person who the personal data is about is known as the data subject and the person who is making the request is known as the applicant. These can of course be the same person depending on the personal data sought. A common example of this relationship would be when a parent (applicant) is seeking personal information about their child (data subject).

10.2.2 To request access to personal data that the Academy holds about a Data Subject, a Subject Access Request (SAR) form can be completed and submitted to the Academy. The form is not a requirement as a valid request does not have to be in a specified format. But for convenience of record keeping the Academy requests that applicants use the form.

10.2.3 Parents may request information about their children. However, the legislation specifies that the rights over personal data rest with the subject of that data, providing that the subject has sufficient maturity and competency to understand their rights. There is no prescribed age specified in the legislation for this, but other parts of the legislation indicate that 13 is a reasonable starting point. This means that:

10.2.3.1 Pupils aged 13 and over will be informed when a request is made, and of their right to refuse to allow disclosure.

10.2.3.2 In the case of any child (including those under the age of 13) refusing to allow disclosure, an assessment must be made of their competency. If a child is assessed as competent then their control over their personal data for these purposes cannot be overridden by the wishes of the parents.

10.2.4 The Academy must take sufficient steps to be satisfied of the identity of the applicant and their right to the information. To these ends, the Academy may request any identification documents reasonably necessary to establish identity. These should only be requested where there is doubt about identity. These will normally include:

10.2.4.1 one piece of photographic identification, such as a valid passport, valid driving licence or a valid EU national identity card.

10.2.4.2 one piece of identification confirming address and dated within the last three months such as a utility bill, council tax statement or bank statement.

10.2.5 There is no fee for a Subject Access Request. Where a request is manifestly unreasonable or excessive then the Academy will opt to refuse the request rather than charge a fee as allowed by the legislation.

10.2.6 The Academy has one calendar month to respond to a subject access request. This may be extended in some circumstances which will be explained at the time they occur.

10.2.7 The details in this policy are a summary only. The Academy will manage Subject Access with due regard to the Information Commissioner's Office Subject Access Code of Practice, and where necessary, in consultation with the Data Protection Officer.

10.2.8 A separate right exists under the Education (Pupil Information) (England) Regulations 2005 (SI 2005/1437) for parents to view their child's Educational

Record free of charge. However, a charge may be made for providing a copy of these documents.

**10.3 Other individual rights**

10.3.1 Further rights provided by the legislation and relevant to the processing carried out by the Academy are:

- Right to rectification
- Right to erasure (Right to be forgotten)
- Right to restrict processing
- Right to object to processing

10.3.2 The Academy will uphold these rights in accordance with the legislation. Individuals wishing to know more about these rights should be referred to the Information Commissioner's Office website. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

10.3.3 To exercise their rights data subjects should contact the Data Protection Officer.

**11. Closed Circuit Television (CCTV)**

11.1 The Academy uses CCTV for the purposes of:

11.1.1 Monitoring entrance to the Academy and allowing office staff to observe visitors.

11.1.2 Security and crime prevention

11.2 CCTV is recorded.

11.2.1 Recordings are only kept for 30 days unless specifically marked for retention. For example, when it is known that an incident has been recorded and the CCTV asset owner decides the footage will be retained.

11.2.2 Footage retained will be kept for as long as necessary to serve the purpose it was retained for and the CCTV manager will review retained footage annually to determine if it is still required and dispose of any that is not, in line with the retention and destruction policy.

**11.3** The Academy's CCTV manager is the Facilities Manager and they are responsible for ensuring CCTV is managed in line with the ICO's CCTV code of conduct.

**12. Information Asset Register**

**12.1** The Academy is required by Article 30 of the GDPR to keep a record of data processing activities. This is maintained in an Information Asset Register.

**12.2** For each Asset listed in the register, there will be specified:

12.2.1 The purposes the information is used for.

12.2.2 The categories of data subjects (e.g. students, parents, staff)

12.2.3 The categories of personal data (e.g. contact details, educational records, employment records)

12.2.4 The retention period for that data, or link to the retention and destruction policy.

12.2.5 Details of any transfers to international organisations or third-party countries.

12.2.6 Security measures protecting the data

12.2.7 The condition(s) under Article 6 and/or Article 9 of the GDPR that allow the processing

12.2.8 The lawful basis relied on for the processing

12.2.9 The details of any joint Data Controllers

12.2.10 The information necessary to demonstrate compliance with any of the other functions referred to in this policy. e.g. sections 4 through 9.

12.2.11 The Information Asset Owner (IAO)

**12.3** The maintenance of this register will be overseen by the Headteacher and the responsibility for ensuring each entry remains accurate and is regularly reviewed lies with the corresponding IAO.

**13. Information Sharing with third parties / joint controllers / processors**

13.1 The Academy shall only share data with third parties when the following conditions are met:

13.1.1 There is a contract in place with specifying how the third party will process data on behalf of the Academy.

13.1.1.1 All contractors are required to meet specified data security standards, and have adequate policies in place.

13.1.2 There is a written Data/Information Sharing Agreement in place with another Data Controller such as the Local Authority or another Academy which describes the responsibilities of both parties.

13.1.3 An exemption applies which allows or requires the Academy to disclose data to that third party (for example, to assist with police investigations or by the order of the courts).

13.1.3.1 Police or other parties asking the Academy to disclose data for these purposes should contact us

13.1.4 Where other conditions set out in regulation 6 and/or regulation 9 of the GDPR apply and permit personal data to be shared. E.g. the subject has given consent.

13.2 The Academy does not store or transfer data outside of the European Union.

**14. Data Breaches**

15.1 Appropriate measures are taken against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data by the Academy. This procedure will be followed in the event of a data security breach, examples of which are:

- Loss or theft of data or equipment on which data is stored on Academy premises or outside
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error - correspondence with personal data sent to the wrong email address
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceit from the Academy

15.2 The Academy will follow the following steps if a data security or potential data security breach occurs:

**1. Detection**

When a member of staff becomes aware that a breach or potential breach has occurred, they must notify the SIRO and DPO as soon as possible.

**2. Containment and recovery**

- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise
- Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause.
- Where appropriate, inform the police
- Assess whether the breach should be reported to the ICO
- Notify the ICO within 72 hours of breach being detected if breach is identified as serious

**3. Assessment of ongoing risk**

The following points are also likely to be helpful in making this assessment:

- What type of data is involved – staff or pupil sensitive personal data
- Where personal data has been lost or stolen, are there any protections in place such as encryption?
- How many staff and/or pupils' personal data are affected by the breach?

- What harm can be done to these individuals – risks to physical safety, reputation etc.

**4. Notification of breach**

The DPO and SIRO will arrange for those affected by the breach to be notified as soon as practically possible.

**5. Evaluation and response**

In the event of a breach, the DPO will complete an investigation as to the causes of the breach and also evaluate the effectiveness of the Academy's response to it. This will be reported to a Committee of the Governing Body and where necessary, the Academy will update its policies and procedures accordingly.

The Academy will maintain a log of breaches, specifying the nature of the incident and the response taken.

## 15. Privacy by design and default, and Data Protection Impact Assessments (DPIA)

**15.1** Whenever the Academy is implementing a new system or business practice that involves the processing of personal data, the Academy will observe privacy by design.

**15.2** A DPIA is a risk-based approach required by the GDPR to identify and manage high risk processing by identifying it and associated risks early.

**15.3** All new projects or systems which involve the processing of personal data require a DPIA screening questionnaire (DPIA pre-screen) to be completed by the project manager.

**15.4** The (DPIA pre-screen shall be submitted to the Academy's management and the DPO, who will advise on the risks and whether a full DPIA is required.

**15.5** For those projects considered to be High Risk, or otherwise requiring a full DPIA, the project manager and the Data Protection Advice Team will prepare the full DPIA for submission to the DPO for approval before the project is able to proceed.

**15.6** The pre-screen and the full DPIA, and associated guidance about how to complete these is available to staff on the Academy intranet/shared drive.

## 16. Photography

16.1 The Academy uses photographs of individuals for the following purposes:

16.1.1 Security and access purposes (ID cards or passes)

16.1.2 To assist staff with the identification of pupils with allergies

16.1.3 Class photographs – records for posterity.

16.1.4 Our own publications – such as newsletters, our website, or the prospectus.

16.1.5 Providing photographs for other media to use in their publications.

**16.2** Consent will be sought for the use of photographs at the start of the Academy year or for listed specific purposes, except where the use of photographs is considered essential to the operation of the Academy or the safety of pupils (sections 17.1.1 and/or 17.1.2)

16.2.1 Where the use of photographs is not within 17.2, specific consent will be sought from the subject as per section 20 below. Pupils aged 13 and over will be presumed to have capacity to consent or not to photographs. Where a pupil is under 13 or does not have capacity, a parent/person with parental responsibility will be asked to consent. Parents cannot override a child's refusal to consent to photography where consent is required, where the child has capacity and is 13 or over.

17. **Telephone Call Recordings**

Only answer phone messages left are recorded. The messages are listened to and then deleted.

17.1 The Academy does not record telephone calls

17.2 Call recordings are stored for a period of no more than 42 days.

**18. Biometrics**

**18.1** Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

**18.2** The Academy does not use biometric data.

18.3 Consent is required for biometrics under the Protection of Freedoms Act in addition to the Data Protection Legislation. This means that consent is required from at least one parent. If one parent objects and the other consents, this shall not be considered consent.

18.4 Consent is also required from the child under Data Protection Legislation (see section 20). Parents may act for the child, but children over the age of 12 may be informed of their right to consent, or not consent, as set out in section 20.

**19. Consent**

19.1 In order to process personal data, the Academy relies primarily on the conditions provided by regulation 6(1)(c) (legal obligation) or 6(1)(e) (public task). The condition provided by 6(1)(a) (consent) will normally only be used when another does not apply.

19.2 When consent is used as the basis for processing, the Academy shall request consent and that request shall:

19.2.1 Be in writing.

19.2.2 Require a positive action to “opt in” or give consent.

19.2.3 Be clear and concise and where consent is being asked of a child; extra care shall be taken to phrase the consent in terms they are likely to understand.

19.2.4 As far as practicable in the circumstances, be specific and granular to avoid blanket consent or any other possible confusion.

19.2.5 Be provided alongside a Privacy Notice. (See section 4.3 of this policy)

19.2.6 Explain how to withdraw consent.

19.2.6.1 It will always be possible for consent to be withdrawn at any time after it has been given, although if the processing has already occurred it may not be possible to reverse that. e.g. If a publication is already printed and distributed, and a subject changes their mind about the use of a photograph, the Academy may only be able to stop the use of that photograph in future publications.

19.3 Processing shall not take place until the consent request has been completed and returned. The consequences of this will be explained in the request.

19.4 Consent from children

19.4.1 The rights provided by the legislation rest with the subject of the data. This means that where the data is about children, and where the child has sufficient maturity and understanding, the child may exercise their right to consent, or withdraw consent, as appropriate. There is no fixed age provided by the

legislation, but as a starting point, children aged 13 years or older will be informed of consent requests and their associated rights.

19.5 The Academy will maintain sufficient records of consent to be able to demonstrate that consent has been given or withdrawn for any processing of personal data relying on consent until that processing has ceased.

**20. Review**

This policy will be reviewed when required by the Academy Business Manager. This policy is subject to as required by developments in case law or guidance issued by the ICO or other official body. Changes may occur without advance notice.