Greig City Academy

Data Protection Policy
2024

"Show by a good life that your works are done
by gentleness born of wisdom."
James 3:13

This policy was approved by the Full Governing Body on July 9, 2024.

This policy will be reviewed in June 2025 or earlier if there are any legislative changes that affect its provisions.

This policy will be published on the Academy's website www.greigcityacademy.co.uk and made available on request to the Exec. PA and HR Manager V. Oxley, in the following formats: e-mail, enlarged print version, others by arrangement.

Greig City Academy
Data Protection Policy

1. Aims

1.1 The Academy aims to ensure that all personal data collected, stored, processed and destroyed about any natural persons whether they be a member of the school workforce, students, parents, governors, visitors or any other individuals is done so in accordance with the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 (DPA 2018) and the Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003.

1.2 This policy applies to all personal data regardless of whether it is in paper or electronic format, or the type of filing system it is stored in, and whether the collection or processing of data was, or is, in any way automated.

2. Legislation and guidance

2.1 This policy meets the requirements of UK Data Protection Legislation. It is based on guidance published by the Information Commissioner's Office (ICO) on the EU GDPR, PECR 2003, UK GDPR and DPA 2018. It is also based on the information provided by the Article 29 Working Party.

2.2 Additionally, it meets the requirements of the Protection of Freedoms Act 2012, ICO's code of practice in relation to video surveillance, and the DBS Code of Practice in relation to handling sensitive information.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity (for example, information about their gender, ethnicity or financial situation)
Special category data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation

	The Academy also processes sensitive information that is not set out in the legislation as 'special category personal data'. This includes information about criminal offences, children's services interactions, free school meal status, pupil premium eligibility, elements of special educational need information, safeguarding information and some behaviour data. Such data will also be treated with the same high status as special categories set out in law.
Processing	Anything done to personal data such as collecting, recording, organising, storing, adapting, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Subject access request	Anybody who makes a request to see personal data held on them or their child is making a subject access request. All information relating to the individual may be considered for disclosure.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

4.1 Greig City Academy collects and determines the processing for data about staff, students, parents and other individuals who come into contact with the school. In addition they process data on the behalf of others therefore are considered a data controller and a data processor.

4.2 Schools have a duty to be registered, as data controllers, with the ICO detailing the information held and its use. The Academy has notified the ICO of its processing activities and these are published on the ICO's website. The Academy's ICO registration number is Z3527658.

5. Roles and responsibilities

5.1 This policy applies to all staff employed by the Academy, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.2 The Governing Body has ultimate responsibility for compliance with data protection law. Governors also have an oversight role in making sure the Academy has good network security to keep personal data protected. This includes having a business continuity plan in place that has cyber resilience as a consideration.

5.3 The Principal acts as the representative of the Governing Body on a day-to-day basis.
The data protection officer (DPO) is responsible for overseeing the implementation of this policy, along with any future development of this or related policies/guidelines and reviewing our compliance with data protection law.

5.4 The school's DPO is:

Paul Letford, Assistant Vice Principal: pletford@greigcityacademy.co.uk
(020) 8609 0100

5.5 The DPO is responsible for:

- promoting a culture of data protection within the Academy.
- advising and training staff about their data obligations.
- monitoring compliance, including managing internal data protection activities.
- conducting annual audits.
- advising when data protection impact assessments are required.
- being the first point of contact for data protection enquiries.
- being the point of contact for the Information Commissioner.
- reporting directly to the Finance and Premises Committee of the Governing Body.

5.7 The DPO is the first point of contact for individuals whose data the school processes, and for the ICO.

5.8 All staff (regardless of their role) are responsible for:

- collecting, storing and processing any personal data in accordance with this policy.
- informing the Academy of any changes in their personal data, e.g., a change of address, telephone number, or bank details.
- Reporting a Data Breach, Data Right Request, or Freedom of Information Request.
- contacting the DPO in the following circumstances:
    - with any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - if they have concerns that the policy is not being followed
    - if they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - if they need to rely on draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the United Kingdom.
    - whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - if they need help with any contracts or sharing personal data with 3rd parties

6. Data protection principles

6.1 Data Protection is based on seven principles with which the Academy must comply. These are that personal data must be:

- processed lawfully, fairly and in a transparent manner .
- 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.
- processed in way that ensure it is appropriately secure.
- kept for no longer than is necessary for the purposes for which it is processed.

6.2 The Accountability principle ties these all together by requiring an organisation to take responsibility for complying with the other six principles. Including having appropriate measures and records in place to be able to demonstrate compliance.

6.3 This policy sets out how the school aims to comply with these key principles.

7. Processing personal data

Lawfulness, fairness and transparency

7.1 The Academy will process personal data only where we have one of these six lawful bases legal reasons) to do so under data protection law:

1. The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract.
2. The data needs to be processed so that the school can **comply with a legal obligation**.
3. The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life.
4. The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest**, and carry out its official functions.
5. The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden).
6. The individual (or their parent/carer when appropriate in the case of a student) has freely given clear **consent.**

7.2 For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in data protection law. These are where:

1. The individual (or their parent/carer, where appropriate) has **given explicit consent.**
2. It is necessary for the purposes of carrying out the **obligations and exercising specific rights** of the controller or of the data subject in the field of **employment** of a Data Controller or of a Data Subject.
3. It is necessary to protect the **vital interests** of the Data Subject.
4. Processing is carried out in the course of its **legitimate activities** with appropriate safeguards by a **foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim.**
5. The Personal Data has **manifestly been made public** by the Data Subject.
6. There is the **establishment, exercise or defence of a legal claim**.
7. There are reasons of **public interest** in the area of **public health**.
8. Processing is necessary for the purposes of preventative or occupational medicine (e.g., for the **assessment of the working capacity of the employee**, the medical diagnosis, the provision of health or social care or treatment).
9. There are **archiving** purposes in the **public interest**.

7.3 Where we collect personal data directly from individuals, we will provide them with the relevant information required by data protection law, in the form of a privacy notice.
These privacy notices can be found in a location accessible and relevant to the data subjects

- Students and Parents/Carers: School website https://www.greigcityacademy.co.uk/396/key-information/category/7/policies
- School Workforce (includes Trainees, Contractors and Consultants): HR Department/school website/staff drive

- Governors & Volunteers: HR Department.
- ***J***ob Applicants: school website https://www.greigcityacademy.co.uk/453/privacy-notice. HR Department.
- Visitors: School reception

Limitation, minimisation and accuracy

7.4 We will collect personal data only for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data via our privacy notices or privacy notifications. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and will seek consent where necessary. Staff must only process personal data where it is necessary in order to fulfil their responsibilities. When staff no longer need the personal data they hold, they must ensure it is destroyed or anonymised. This will be done in accordance with the Academy's Data retention schedule, which states how long particular data and documents should be kept, and how they should be destroyed. This document is line with the Information and Records Management Society's guidance for schools.

7.5 Copies of the Data Retention schedule can be obtained by contacting Viv Oxley, Exec PA and HR Manager: 020 8609 0175; voxley@greigcityacademy.co.uk.

8. Biometric recognition systems

8.1 Where we use students' biometric data as part of an automated biometric recognition system (for example, use of fingerprints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

8.3 Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

8.4 Parents/carers and students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those students.

8.5 Parents/carers and students can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

8.6 As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the students' parent(s)/carer(s).

9. Sharing personal data

9.1 In order to efficiently, effectively and legally function as a data controller we are required to share information with appropriate third parties, including but not limited to situations where:

- there is an issue with a student or parent/carer that puts the safety of our staff at risk.
- we need to liaise with other agencies or services – we may seek consent when appropriate before doing this where possible.
- our suppliers or contractors need data to enable us to provide services to our employees and pupils – for example, IT companies. When doing this, we will:

- only appoint suppliers or contractors that can provide sufficient guarantees that they comply with data protection law and have satisfactory security measures in place.
- establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
- only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

9.2 We will also share personal data with law enforcement and government bodies when required to do so, these include but are not limited to:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

9.3 We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or employees.

9.4 The Academy is required by law to pass some information about students to the Department for Education (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013. We share information with other agencies prescribed by law, such as the Qualifications and Curriculum Authority (QCA), Ofsted, the Education and Skills Funding Agency (ESFA), the Department of Health (DH). We are also required to pass a student's personal data to any school to which s/he transfers.

10. Confidentiality of student concerns

10.1 Where a student raises concerns with a member of staff and expressly withholds agreement to their personal data being disclosed to their parents/guardian, the Academy will maintain confidentiality unless it has reasonable grounds to believe that the student does not fully understand the consequences of withholding their consent, or where the Academy believes disclosure will be in the best interests of the student or other students.

11. Transferring Data Internationally

11.1 We may send your information to other countries where:

- we or a company with which we work store information on computer servers based overseas; or
  we communicate with you when you are overseas.

11.2 We conduct due diligence on the companies we share data with and note whether they process data in the UK, EEA (which means the European Union, Liechtenstein, Norway and Iceland) or outside of the EEA.

11.3 The UK and countries in the EEA are obliged to adhere to the requirements of the GDPR and have equivalent legislation which confer the same level of protection to your personal data.

11.4 For organisations who process data outside the UK and EEA we will assess the circumstances of how this occurs and ensure there is no undue risk.

11.5 Additionally, we will assess if there are adequate legal provisions in place to transfer data outside of the UK

12. Individuals' Data Rights

Access rights

12.1 Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them. If you make a subject access request, and if we do hold information about you, we can:

- give you a description of it.
- tell you why we are holding and processing it, and how long we will keep it for.
- explain where we got it from, if not from you.
- tell you who it has been, or will be, shared with.
- let you know whether any automated decision-making is being applied to the data, and any consequences of this.
- NOT provide information where it compromises the privacy of others.
- give you a copy of the information in an intelligible form.

12.2 When responding to requests, we will not disclose information if it:

- might cause serious harm to the physical or mental health of the student or another individual; or
- would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests; or
- is contained in adoption or parental order records; or
- is given to a court in proceedings concerning the child; or
- would include another person's personal data that we cannot reasonably anonymise, and we do not have the other person's consent and it would be unreasonable to proceed without it; or
- is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

Other Rights regarding your data

12.3 You may also:

- withdraw your consent to processing at any time; this relates only to tasks where the school relies on consent to process the data.
- ask us to rectify, erase or restrict processing of your personal data, or object to the processing of it in certain circumstances and where sufficient supporting evidence is supplied.
- prevent the use of your personal data for direct marketing.
- challenge processing which has been justified on the basis of public interest, official authority or legitimate interests.
- request a copy of agreements under which your personal data is transferred outside of the United Kingdom.

- object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them).
- request a cease to any processing that is likely to cause damage or distress.
- be notified of a data breach in certain circumstances.
- refer a complaint to the ICO.
- ask for your personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

12.4 In most cases, we will respond to requests within 1 month, as required under data protection legislation However, we are able to extend this period by up to 2 months for complex requests or exceptional circumstances.

12.5 We reserve the right to verify the requesters identification by asking for Photo ID, if this proves insufficient then further ID may be required.

12.6 If the request is manifestly unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which would only take into account administrative costs.

12.7 A request will be deemed to be manifestly unfounded or excessive if it is repetitive or asks for further copies of the same information.

12.8 In the event we refuse a request, we will tell the individual why, and tell them they have the right to refer a complaint to the ICO.

12.9 The School will comply with the Data Protection legislation in regard to dealing with all data requests submitted in any format. However, people are asked preferably to submit their request in writing to assist with comprehension.

12.10 Requests should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the request

12.11 If you would like to exercise any of the rights or requests listed above, please contact:

Paul Letford, DPO
Greig City Academy, High Street, Hornsey, London, N8 7NU
E: pletford@greigcityacademy.co.uk
T: 020 8609 0148

12.12 If staff or volunteers receive a subject access request, they must immediately forward it to the DPO, Paul Letford – details as above.

<u>Children and requests</u>

12.13 An individual's data belongs to them therefore a child's data belongs to that child, and not the child's parents or carers.

12.14 Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of invoking a data request. Therefore, for children under the age of 12 most data requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

12.15 Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our school may not be granted without the express permission of the pupil. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

13. CCTV

13.1 We use CCTV in various locations around the school sites and premises for the detection and prevention of crime. We adhere to the ICO's code of practice for the use of video surveillance and provide training to staff in its use.

13.2 We do not need to ask individuals' permission to use CCTV, but in most instances, we make it clear where individuals are being recorded, with security cameras that are clearly visible and accompanied by prominent signs explaining that CCTV is in use, and where it is not clear, directions will be given on how further information can be sought.

13.3 Any enquiries about the CCTV system should be directed to Peter Law, Premises Manager: E: plaw@greigcityacademy.co.uk; T: 020 8609 0140.

14. Consent for promotional purposes, photographs/recordings

14.1 The Academy may make use of limited personal data (such as contact details) relating to students, their parents or guardians for promotional purposes and to maintain relationships with students and alumni, but only where consent has been freely provided.

14.2 When a student joins the Academy, both the student and the parent are asked to sign a consent form for photographs to be taken/recordings to be made for use in Academy publications, displays, its website and social media sites. 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.

14.3 You can withdraw consent by contacting the DPO, Paul Letford, Assistant Vice Principal: T: 020 8609 0148; E: platford@greigcityacademy.co.uk.

14.4 Where the media or organisations running events for student groups request photographs and names of students for promotional or congratulatory purposes, consent specifically for that purpose will be requested from students and, where appropriate, parents.

14.5 See our Online Safety Policy for more information on the use of photographs/recordings.

15. Artificial intelligence (AI) Artificial intelligence

15.1 AI tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. The School recognises that AI has many uses to help students learn, but also poses risks to sensitive and personal data. To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots. If personal and/or sensitive data is entered into an unauthorised generative AI tool, the school will treat this as a data breach, and will follow the personal data breach procedure outlined in this policy.

16. Data protection by design and default

16.1 We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Providing regular training for the school workforce and volunteers on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Periodically conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO, and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

17. Data security and storage of records

17.1 We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

17.2 Paper-based records and portable electronic devices such as laptops and hard drives that contain personal data are kept under lock and key when not in use.

17.3 Staff are made aware that papers containing confidential personal data must not be left anywhere where there is general access.

17.4 Where personal information needs to be taken off site in paper form a note will be left in the file from which it has been taken, stating when it was taken and by whom. The file will be signed in again when returned. Whilst off-site the documents are the responsibility of the member of staff who took them and should be kept in an opaque folder and, where possible, on the person at all times.

17.5 Where personal information is taken off site in electronic form, encryption software will be used to protect portable devices and removable media.

17.6 Where personal information needs to be sent by email this should be as a password protected file and the password shared by different message by text or by phone call.

17.7 Where information is held on laptops/tablets that travel between school and home, both the device and the files must be password protected.

17.8 Staff, students and governors who store personal information on their personal devices must follow the same security procedures as for school-owned equipment.

17.9 Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

18. Disposal of records

18.1 Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will be rectified or updated, unless it is no longer of use and therefore will be disposed of securely.

18.2 For example, we will shred paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law and provide a certificate of destruction.

18.3 When records are disposed of as part of the Data Retention schedule this is then recorded on our record of destruction log.

19. Personal data breaches

19.1 The Academy will make all reasonable endeavour to ensure there are no personal data breaches.

19.2 All potential or confirmed Data Breach incidents should be reported to the DPO, Paul Letford, who will assign a unique refence number and make a record in the school's data breach log.

19.3 Once logged, incidents will be investigated, the potential impact assessed, and appropriate remedial action undertaken.

19.4 Where appropriate, we will report the data breach to the ICO and affected Data Subjects within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of students eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about students

20. Training

20.1 All staff and governors will be provided with data protection awareness training as part of their induction process. Data protection awareness will also form part of CPD, including when changes to legislation, guidance or the Academy's processes make it necessary.

21. Monitoring

21.1 This policy will be reviewed annually by the DPO, and changes recommended where appropriate. The Governing Body will be asked to approve the policy review and any necessary changes.

22. Contacts

22.1 If anyone has any concerns, comments, complaints or questions in relation to this policy, they should contact:

Paul Letford, Data Protection Officer, 020 8609 0148 or pletford@greigcityacademy.co.uk.

22.2 If anyone is unhappy with the response from the school, they have the option of complaining to, or getting advice from:

Information Commissioner's Office (ICO)
https://ico.org.uk
Telephone: 0303 123 1113 or Textphone: 01625 545 860

23. Links with other policies

Safeguarding and child protection policy
Health and safety policy
Online safety policy
Acceptable use policy
Freedom of information publication scheme
Privacy notices: students and parents; staff; governors; contractors and suppliers