Data Protection Policy

Date/Version : April 2024. V3

Table of Contents

Table of Contents
1. Introduction
    1.1 Legislation and guidance
    1.2 Definitions
        TERM
        DEFINITION
    1.3 The Data Controller
    1.4 Roles and responsibilities
        1.4.1 Grow Education Partners Board
        1.4.2 Data Protection Officer
        1.4.3 Data Controller Representative
        1.4.4 Employees
    1.5 The Data protection principles
    1.6. Processing personal data
        1.6.1 Lawfulness, fairness and transparency
        1.6.2 Limitation, minimisation and accuracy
    1.7 Sharing personal data
    1.8 Transferring Data Internationally
    1.9 Artificial intelligence (AI)
    1.10 Individuals rights under GDPR
        1.10.1 Access Rights
        1.10.2 Other Rights regarding your Data:
    1.11 Children and Data Rights Requests
    1.12 Photographs and videos
    1.13 Data protection by design and default
    1.14 Data security and storage of records
    1.15 Disposal of records
    1.16 Personal data breaches
    1.17 Monitoring arrangements
    1.18 Links with other policies

1. Introduction

Grow Education Partners aims to ensure that all personal data collected, stored, processed and destroyed about any natural person, whether they be a Board Member, supporter, consultant, visitor, contractor, a Grow Education Partners employee or any other individual 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.

This policy applies to all personal data processed by the school, 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.

1.1 Legislation and guidance

This policy meets the current 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. It also meets the requirements of the Protection of Freedoms Act 2012, and the DBS Code of Practice in relation to handling sensitive information.

1.2 Definitions

TERM	DEFINITION
Data controller	The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data processor	A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller, following the Controller's instruction.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Consent	Freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a ● name, ● an identification number, ● location data, ● an online identifier or ● to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Special categories of personal 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 • history of offences, convictions, or cautions * * Note: whilst criminal offences are not classified as "sensitive data" within GDPR, within this policy template we have included them as such as acknowledgement of the care needed with this data set.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing can be automated or manual.
Data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

1.3 The Data Controller

Grow Education Partners collects and determines the use of personal data relating to employees, Board Members and other categories data subjects, in addition they process data on the behalf of others and therefore is a data controller. and a data processor.

Grow Education Partners is registered as a data controller with the ICO and will renew this registration as legally required, the registration number is ZB046765.

1.4 Roles and responsibilities

This policy applies to all individuals employed by Grow Education Partners, and to external organisations or individuals working on our behalf. Employees who do not comply with this policy may face disciplinary action.

1.4.1 Grow Education Partners Board

The Grow Education Partners Board has overall responsibility for ensuring that Grow Education Partners complies with all relevant data protection obligations.

1.4.2 Data Protection Officer

Our Data Protection Officer (DPO) is David Coy (david.coy@london.anglican.org, 020 3837 5145).

They are responsible for overseeing the implementation of this policy in the first instance, before reviewing our compliance with data protection law, and developing related policies and guidelines where applicable.

Upon request our DPO will provide an annual report of Grow Education Partners' compliance and risk issues directly to the Grow Education Partners Board and will report to the board their advice and recommendations on data protection issues.

Our DPO is also a point of contact for individuals whose data Grow Education Partners processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

1.4.3 Data Controller Representative

The Managing Director acts as the representative of the data controller on a day-to-day basis.

1.4.4 Employees

All employees (regardless of role) are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing Grow Education Partners of any changes to their personal data, e.g. a change of address, telephone number, or bank details.
- Reporting a Data Breach or Data Right Request.
- Contacting the DPO:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, 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 third parties

1.5 The Data protection principles

Data Protection is based on seven principles that Grow Education Partners must comply with. These are that data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.

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.

This policy sets out how Grow Education Partners aims to comply with these key principles.

1.6. Processing personal data

1.6.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of six 'lawful bases' (legal reasons) to do so under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent.
- The data needs to be processed so that Grow Education Partners can fulfil a contract with the individual, or the individual or client has asked Grow Education Partners to take specific steps before entering into a contract.
- The data needs to be processed so that Grow Education Partners can comply with a legal obligation.
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life.
- The data needs to be processed for the legitimate interests of Grow Education Partners or a third party (provided the individual's rights and freedoms are not overridden)

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:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent.
- 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
- It is necessary to protect the vital interests of the data subject.
- 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.
- The personal data has manifestly been made public by the data subject.
- There is the establishment, exercise or defence of a legal claim.
- There are reasons of public interest in the area of public health.
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment.
- There are archiving purposes in the public interest.

Whenever we first 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, which can be found on the Grow Education Partners website.

Additional copies are available on request.

1.6.2 Limitation, minimisation and accuracy

- We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data via our privacy notices.
- 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 seek consent where necessary.
- Employees must only access and process personal data where it is necessary to do their jobs.
- We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.
- When personal data is longer required, employees must ensure it is destroyed. This will be done in accordance with the school data retention policy, which states how long particular documents should be kept, and how they should be destroyed.

Copies of the Data Retention Policy can be obtained by contacting the DPO via

- Email: david.coy@london.anglican.org,
- Phone: 020 3837 5145,
- Address: Grow Education Partners, London Diocesan House, 36 Causton Street, London, SW1P 4AU

1.7 Sharing personal data

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:

- We need to liaise with other agencies or services – we may seek consent when appropriate before doing this where possible.
- Our suppliers, consultants or contractors need data to enable us to provide services to our staff or service users – for example, IT companies. When doing this, we will:
  - Only appoint suppliers, consultants or contractors which 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, consultant, 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, consultant, or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so for:

- 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.

We may also share personal data with emergency services and other authorities to help them to respond to an emergency situation that affects any of our staff as well as service users while they are on site.

1.8 Transferring Data Internationally

We may send your information to other countries where:

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

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.

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.

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.

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

1.9 Artificial intelligence (AI)

(AI) tools are now widespread and easy to access. Employees may be familiar with generative chatbots such as ChatGPT and Google Bard. We recognise that AI has many uses to help individuals with their work, 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. We will treat this as a data breach, and will follow the personal data breach procedure outlined in this policy

1.10 Individuals rights under GDPR

1.10.1 Access Rights

Individuals have a right to make a 'subject access request' to gain access to personal information that we hold 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.

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

- Might cause serious harm to the physical or mental health of the pupil 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

1.10.2 Other Rights regarding your Data:

You may also:

- Withdraw their consent to processing at any time, this only relates to tasks which 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)

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.

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

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.

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

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.

We will comply with the Data Protection legislation in regard to dealing with all data requests submitted in any format, individuals are asked to preferably submit their request in written format to assist with comprehension.

They should include:

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

If you would like to exercise any of the rights or requests listed above, please contact our DPO, David Coy

- Email: david.coy@london.anglican.org
- Phone: 020 3837 5145
- Address: Grow Education Partners, London Diocesan House, 36 Causton Street, London, SW1P 4AU

If an individual receives a requests, they must immediately forward it to the DPO, David Coy

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

- Might cause serious harm to the physical or mental health of the pupil 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

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.

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

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.

1.11 Children and Data Rights Requests

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

However, children below the age of 12 are generally not regarded as 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 pupil's ability to understand their rights will always be judged on a case-by-case basis.

Where a child is judged to be of sufficient age and maturity to exercise their rights and a request is invoked on their behalf, we would require them to give consent to authorise the action to be undertaken.

1.12 Photographs and videos

We receive photographs and videos from time to time from schools, authorising bodies and events where children are present.

All photographs and videos are personal data for data subjects and consent for their use should be followed carefully within our rules and procedures for data security and storage of records detailed at point 1.11. below.

We will protect all photographs and videos and keep them safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

1.13 Data protection by design and default

We will put measures in place to show that we have integrated data protection into all our data collection and processing activities. These include, but are not limited to the following organisational and technical measures:

- 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 regulations.
- Completing data privacy impact assessments where Grow Education Partners' processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies or processing tools. Advice and guidance will be sort from the DPO.
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Providing regular training members for employees and Board Members on data protection law, this policy and any related policies and any other data protection matters. Records of attendance will be kept to record the training sessions, and ensure that all data handlers receive appropriate training.
- Periodic 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 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, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

1.14 Data security and storage of records

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. Our organisational and technical measures include but are not limited to.

- Paper-based records and portable electronic devices, such as laptops, tablets and hard drives that contain personal data will be kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.
- Passwords that are at least eight characters long containing letters and numbers are used to access Grow Education Partners computers, laptops, and other electronic devices. Staff are reminded to change their passwords at regular intervals. Multi-factor authentication will be used when available.
- Encryption software is used to protect any devices such as Laptops, Tablets and USB Devices where saving to the hard drive is enabled.
- Employees, consultants, contractors, or Board Members, who store personal information on their personal devices are expected to follow the same security procedures as for Grow Education Partners-owned equipment (see Grow Education Partners' ICT, User Agreements for further information)
- 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.

1.15 Disposal of records

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.

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.

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

1.16 Personal data breaches

Grow Education Partners will make all reasonable endeavours to ensure that there are no personal data breaches.

All potential or confirmed Data Breach incidents should be reported to the DPO, David Coy where they will be assigned a unique reference number and recorded in the school's data breach log.

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

Where appropriate, we will report the data breach to the ICO within 72 hours. The full procedure is set out in the Breach Management Policy

Examples of Data Protection breaches may include, but are not limited to:

- A non-anonymised dataset being published on Grow Education Partners website which shows the exam results of pupils eligible for the pupil premium.
- Safeguarding information being made available to an unauthorised person.

- The theft of a Grow Education Partners laptop containing non-encrypted personal data about pupils

1.17 Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy as part of the general monitoring and compliance work they carry out.

They will work with the Managing Director and the Board to ensure that this policy remains contemporaneous and appropriate

1.18 Links with other policies

This data protection policy is linked to the following policies:

- ICT User Agreements
- Document Retention Schedule.
- Breach Management policy
- Asset Management Recording policy
- Disaster Recovery/Business Continuity Planning and Risk Register
- Safeguarding and Child Protection policy