Primus Education

Privacy and Data Protection Policy

Contents

Aims

Primus Education is committed to protecting the privacy and personal data of students, parents/carers, staff, tutors, visitors and other individuals in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and relevant guidance issued by the Information Commissioner's Office (ICO).

Legislation and guidance

This policy has been developed in accordance with relevant data protection legislation and guidance, including:

- **UK General Data Protection Regulation (UK GDPR)**
- **Data Protection Act 2018**
- guidance issued by the **Information Commissioner's Office (ICO)**

This policy applies to all personal data processed by Primus Education, whether held electronically or in paper form.

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.
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 • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, 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.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Data Controller

Primus Education processes personal data relating to parents, students, staff, visitors and others. It is therefore considered to be a data controller.

Responsibility

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

Directors

The directors are fully responsible in ensuring all stakeholders comply with all relevant data protection obligations.

Data Protection Lead

The Data Protection Lead (DPL) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. The DPL is also the first point of contact for individuals whose data is processed by the tuition centre.

All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy.
- Informing Primus Education of any changes to their personal data, such as a change of address.
- Contacting the DPL 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 any concerns that this 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.
    - 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.

Data protection principles

The GDPR is based on data protection principles that Primus Education must comply with. The principles state that personal 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.

This policy sets out how Primus Education aims to comply with these principles.

Collecting Personal Data

Lawfulness, Fairness and Transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that Primus Education can fulfil a contract with the individual, or the individual has asked the us to take specific steps before entering into a contract.
- The data needs to be processed so that the tuition centre 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 Primus Education or a third party (provided the individual's rights and freedoms are not overridden).
- The individual (or their parent/carer when appropriate in the case of a student) has freely given clear consent.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

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. 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.

Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

Sharing Personal Data

We will not normally share personal data with anyone else, but may do so 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 – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
    - 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.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including 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 within the Data Protection Policy.
- 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 local authorities to help them to respond to an emergency situation that affects any of our students or staff.

Subject Access Requests and Other Rights of Individuals

Subject Access Requests

Individuals have the right to request access to the personal information that Primus Education holds about them.

This is known as a **Subject Access Request (SAR)**.

Individuals may request:

- confirmation that their personal data is being processed;
- access to a copy of their personal data;
- information about how and why their data is processed;
- details of who their data may be shared with;
- how long their data is expected to be retained;
- information about the source of data, where this has not been obtained directly from the individual.

Subject Access Requests should be submitted in writing by email or letter to Primus Education.

Requests should include:

- the name of the individual making the request;
- a correspondence address and contact details;

- sufficient detail to identify the information requested.

Primus Education may request proof of identity before releasing information in order to protect personal data and ensure information is disclosed only to the appropriate person.

Primus Education will normally respond to Subject Access Requests **within one calendar month** of receipt of a valid request.

Where requests are particularly complex or involve large amounts of information, Primus Education may extend this period in accordance with UK GDPR requirements. In such circumstances, the individual will be informed of the reason for the delay.

Primus Education will normally provide information free of charge. However, a reasonable fee may be charged where requests are manifestly unfounded, excessive or repetitive.

Requests Made on Behalf of Children

Personal data relating to a child belongs to that child.

Where a parent or carer requests access to information relating to their child, Primus Education will consider the child's age, understanding and best interests when determining whether information can be disclosed.

For younger children, requests from parents/carers will generally be considered appropriate. For older children and young people, Primus Education may seek the child's consent where appropriate.

Primus Education reserves the right to withhold information where disclosure may:

- place a child or another individual at risk of harm;
- compromise safeguarding concerns or investigations;
- breach the rights or confidentiality of another individual;
- be restricted by law.

Other Data Protection Rights

Under UK GDPR, individuals may also have the right to:

- request correction of inaccurate personal data;
- request deletion of personal data in certain circumstances;
- restrict or object to the processing of personal data;
- withdraw consent where consent has been relied upon;
- request transfer of personal data to another organisation where applicable;
- make a complaint to the Information Commissioner's Office (ICO).

Requests relating to personal data rights should be submitted to Primus Education in writing.

Photographs, Videos and Lesson Recordings

Primus Education may, from time to time, take photographs or video content for educational, communication, promotional or marketing purposes.

Where photographs or videos are used for promotional purposes, including on the Primus Education website, social media platforms, printed materials or marketing communications, appropriate consent will be obtained in advance from parents/carers or students aged 18 and over.

Consent may be withdrawn at any time, and Primus Education will take reasonable steps to cease future use of the relevant content.

Where photographs or videos are used, Primus Education will seek to ensure that children and young people are represented appropriately and safely and that unnecessary personal information is not shared.

Online Lesson Recordings

As part of Primus Education's safeguarding, quality assurance and educational provision, online lessons may be recorded.

Lesson recordings may be used for:

- safeguarding purposes;
- quality assurance and professional monitoring;
- tutor training and development where appropriate;
- resolving concerns or disputes relating to tuition delivery.

Lesson recordings will:

- be stored securely using approved Primus Education systems;
- only be accessible to authorised personnel where necessary;
- be handled in accordance with safeguarding and data protection requirements;
- not be shared externally unless there is a lawful basis to do so.

Lesson recordings are treated separately from promotional photographs or marketing content and do not require separate media consent where recordings are undertaken for safeguarding, educational or legitimate operational purposes.

Primus Education will ensure that all recordings are retained only for as long as reasonably necessary and are disposed of securely in accordance with data protection requirements.

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. In particular:

- 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.
- 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.
- Where personal information needs to be taken off site, staff must sign it in and out with an authorised member of Primus leadership.
- Strong passwords and multi-factor authentication where appropriate are used to access on-site computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff, students or trustees or governors who store personal information on their personal devices are expected to follow the same security procedures as for Primus-owned equipment.
- 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.

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 also be disposed of securely, where we cannot or do not need to rectify or update it. 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 Primus' behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Personal Data Breaches

Primus Education will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches may include, but are not limited to:

- A non-anonymised dataset being published on our website which shows the test performance of students eligible for the student premium.
- Safeguarding information being made available to an unauthorised person.
- The theft of a Primus computer device containing non-encrypted personal data about students.

Training

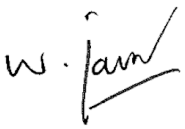
All staff are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or Primus Education's processes make it necessary.

Monitoring arrangements

The DPL is responsible for monitoring and reviewing this policy. This policy will be reviewed annually, or sooner where necessary to reflect changes in legislation, guidance or Primus Education operational practices.

Data Protection Policy Approval

This policy was reviewed and approved by the directors on 16th May 2026.

Signed: 

Date: 16th May 2026

Appendix 1: Personal Data Breach Procedure

Primus Education will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out below:

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPL.
- The DPL will investigate the report, and determine whether a breach has occurred. To decide, the DPL will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed o Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPL will alert the Directors.
- The DPL will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.
- The DPL will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPL will work out whether the breach must be reported to the ICO. This must be judged on a caseby-case basis. To decide, the DPL will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination o Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation o Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned If it's likely that there will be a risk to people's rights and freedoms, the DPL must notify the ICO.
- The DPL will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Primus Education computer system.
- Where the ICO must be notified, the DPL will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPL will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPL
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- If all the above details are not yet known, the DPL will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPL expects to have further information. The DPL will submit the remaining information as soon as possible Data is available.

- The DPL will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPL will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPL
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.
- The DPL will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPL will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored on Primus Education's computer system.
- The DPL and Directors will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

For example: *Sensitive information being disclosed via email (including safeguarding records)*

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the DPL as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the DPL attempt to recall it.
- In any cases where the recall is unsuccessful, the DPL will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPL will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPL will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.