GDPR Policy

Date of review **Reviewed By** **Date of next review**	July 2024 Kath Barclay July 2025

Aims

Bridge the Gap Malvern aims to ensure that all personal data collected about staff, students, parents, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO). It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

This policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living 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 • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • 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.

The Data Controller
Bridge the Gap Malvern processes personal data relating to parents/carers, students, staff, visitors and others, and therefore is a Data Controller.

Roles and responsibilities
This policy applies to all staff employed by our centre, 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 have overall responsibility for ensuring that our centre complies with all relevant data protection obligations.

Data Processing Lead
The Data Processing 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 the first point of contact for individuals whose data the centre processes, and for the ICO.

Full details of the DPL's responsibilities are set out in their role descriptor (appendix 2).

Head of Centre
The Head of Centre acts as the representative of the Data Controller on a day-to-day basis.

All staff
Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the centre of any changes to their personal data, such as a change of address

Staff are responsible for 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
- 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 UK
- If there has been a data breach

- 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 UK GDPR is based on data protection principles that our centre must comply with. The principles say 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 the centre aims to comply with these principles.

Collecting personal data - 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:

1. The data needs to be processed so that the centre can **fulfil a contract** with the individual, or the individual has asked the centre to take specific steps before entering into a contract
2. The data needs to be processed so that the centre can **comply with a legal obligation**
3. The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life
4. The data needs to be processed so that the centre, as a public authority, can **perform a task in the public interest or exercise its official authority**
5. The data needs to be processed for the **legitimate interests** of the centre (where the processing is not for any tasks the centre performs as a public authority) 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**

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

1. The individual (or their parent/carer when appropriate in the case of a student) has given **explicit consent**
2. The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
3. The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
4. The data has already been made **manifestly public** by the individual

5. The data needs to be processed for the establishment, exercise or defence of **legal claims**
6. The data needs to be processed for reasons of **substantial public interest** as defined in legislation
7. The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
8. The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
9. The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

1. The individual (or their parent/carer when appropriate in the case of a student) has given **consent**
2. The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
3. The data has already been made **manifestly public** by the individual
4. The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
5. The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law. See Privacy Statements. We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

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.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the centre's record retention schedule.

Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a student or parent/carer that puts the safety of staff or students 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 sharing personal data with suppliers or contractors, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law
- Establish a contract with the supplier or contractor 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

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

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.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

Subject access requests and other rights of individuals

Individuals have a right to make a 'subject access request' to gain access to personal information that the centre holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority

- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

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

If staff receive a subject access request in any form they must immediately forward it to the DPL.

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

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 centre may not be granted without the expressed permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the student or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests

- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- 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

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

Other data protection rights of the individual
In addition to the right to make a subject access request, and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPL. If staff receive such a request, they must immediately forward it to the DPL.

Parental requests to see the educational record
Parents and carers do not have an automatic right of access to educational records from an independent centre. However, parents, or those with parental responsibility, may request access to their child's educational record (providing they are under 18, or 24 with EHCP).

The centre will aim to comply with the request within 15 centre days of receipt of a written request. There will be an administration fee to cover the cost of supplying it.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the student or another individual.

Photographs and videos
As part of our centre activities, we may take photographs and record images of individuals within our centre.

We will obtain written consent from parents/carers (or students where appropriate) for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at centre events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other students are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or students where appropriate) have agreed to this.

Uses for photographs and videos may include:

- Within the centre on notice boards and in centre newsletters, brochures, etc.
- Outside of the centre by external agencies such as newspapers, campaigns
- Online on our centre website or social media pages

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.

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

We will also obtain written consent from parents/carers (or students where appropriate) for recording remote mentoring and teaching sessions. These will be kept for the following purposes:

- Within centre for safeguarding purposes
- Within centre for quality assurance purposes

Data protection by design and default
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 DPL

- 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
- Completing data protection impact assessments where the centre's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPL will advise on this process)
- Integrating data protection into any related policies and privacy notices
- Keeping staff up to date on this, any related policies
- Conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply

When maintaining records of our processing activities, we will ensure this is:

- For the benefit of data subjects, making available the name and contact details of our DPL 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

Data security and storage of records
Refer to the Data Security & Safety Policy.

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, shredding or incinerating paper-based records, and overwriting or deleting electronic files.

Personal data breaches
The centre 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 after becoming aware of it. Such breaches may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person
- The theft of a centre laptop containing non-encrypted personal data about students

Training
All staff are provided with data protection training as part of their induction process.

Monitoring arrangements
The DPL is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the Directors.

Links with other policies
This data protection policy is linked to our:

- Privacy Statements
- Data Security & Safety Policy
- Remote and E-learning Policy
- E-Safety Policy

Appendix 1
Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the data processing lead (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
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

Staff will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.

If a breach has occurred or it is considered to be likely that is the case, the DPL will alert the Head of Centre and Directors.

The DPL will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPL with this where necessary, and the DPL should take external advice when required (See the actions relevant to specific data types at the end of this procedure)

The DPL will assess the potential consequences (based on how serious they are or how likely they are to happen) before and after the implementation of steps to mitigate the consequences

The DPL will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool

The DPL will document their decision either way, in case the decisions are challenged at a later date by the ICO or an individual affected by the breach.

Where the ICO must be notified, the DPL will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the centre's awareness of the breach. 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, and 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 of the centre's awareness of the breach. 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

Where the centre is required to communicate with individuals whose personal data has been breached, the DPL will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
- 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 consider, in light of the investigation and any engagement with affected individuals, whether to 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)

The DPL and Head of Centre will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

The DPL and Head of Centre will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the centre to reduce risks of future breaches.

Actions to minimise the impact of data breaches
We have set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, 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.

Sensitive information being disclosed via email (including safeguarding records)
If 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 will ask the centre's IT support (iCT4 Limited) to attempt to recall it from external recipients and remove it from the centre's email system (retaining a copy if required as evidence).

In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPL will consider whether it's appropriate to 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 endeavor to obtain 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.

If safeguarding information is compromised, the DPL will inform the Designated Safeguarding Officer and discuss whether the centre should inform any, or all, of its safeguarding partners.

Other types of breach could include, but are not limited to:

- A centre laptop containing non-encrypted sensitive personal data being stolen or hacked
- Hardcopy reports sent to the wrong students or families

Appendix 2

Role Descriptor - Data Processing Lead

Main Purposes

- To ensure compliance with the requirements of General Data Protection Regulation (GDPR)
- To advise staff and managers in relation to GDPR
- Monitoring compliance with GDPR
- Assist the Data Controller with carrying out a data protection impact assessment
- Taking a risk-based approach to data protection
- Be the lead contact for all data protection queries with regard to potential complaints and breaches, ensuring that requests for information are properly handled.

Main Duties and Responsibilities

- Undertake training relevant to the role
- Ensure GDPR non-compliance is recorded on the centre's risk register and notified to line manager promptly
- Production and/or review of key policies and procedures
- Audit compliance with policies and procedures as required
- Keep all staff informed of key strategies, procedures, and changes to the GDPR policy
- Maintain a data audit map to map data flows and share as necessary
- Undertake Data Protection Impact Assessments as required
- Prepare and administer privacy statements as required
- Manage the process for detecting, reporting and investigating data breaches
- Notify individuals whose data has been breached and where it is likely to result in a high risk to their rights and freedoms
- To provide reports as requested by the Head of Centre or Directors

Other Responsibilities

- Maintain the positive ethos and core values of the centre

- Communicate and consult with parents/carers of all students as necessary
- Communicate and cooperate with persons or bodies outside the centre as necessary
- Participate in meetings arranged for any of the purposes outlined above
- Participate in arrangements for further training and professional development as necessary
- To undertake any other relevant duties as deemed appropriate by the Head of Centre

Personal Characteristics

- Good personal communication skills and the ability to deal with a range of stakeholders
- A systematic and meticulous approach to procedures and regulation