FIRST BRIDGE SCHOOL

Data protection policy

Reviewed: March 2026
Next Review: August 2026

Key Information

- **First Bridge Group Ltd is registered with the ICO as a Tier 2 data controller: ZB532576.**

- **The Data Compliance Officer is the People Strategy Manager, Mr Bash Nawaz.**

- **This policy complies with the requirements set out in the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR).**

Introduction

- First Bridge Group Ltd (which runs First Bridge School and both 'First Bridge Group Ltd' and 'First Bridge School' are used interchangeably throughout this policy) is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the UK General Data Protection Regulation (UK GDPR).

- This policy is in place to everybody working at and with First Bridge Group Ltd is aware of their responsibilities, and outlines how the organisation complies with the core principles of the UK GDPR.

- We may, from time to time, be required to share personal information about our staff or pupils with other organisations, such as placing local authorities, other schools and educational bodies, and potentially social care services and the police.

Personal Data

- Personal information is any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips or as sound recordings.

- Personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, such as an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according

to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

- Sensitive personal data is referred to in the UK GDPR as 'special categories of personal data'. These specifically include the processing of genetic data, biometric data and data concerning health matters

- First Bridge School collects personal data in relation to staff and pupil records. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of placing local authorities, government agencies and other bodies.

Principles

In accordance with the requirements outlined in the UK GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.

- 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; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- First Bridge Group Ltd takes technical and organisational measures to demonstrate that data is processed in line with the principles set out in

the UK GDPR.

- Records of activities relating to higher-risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

Data Compliance Officer

Under the UK GDPR, a data controller will only be required to appoint a Data Protection Officer if any of the below three conditions are met:

1. The processing is carried out by a 'public authority'.

2. The 'core activities' require regular and systematic monitoring of data subjects on a 'large scale'.

3. Where 'core activities' involve 'large scale' processing of 'special categories' of personal data and relating to criminal convictions and offences.

For First Bridge Group Ltd, none of these conditions are met, as outlined below, and therefore the school is not required to appoint a DPO.

- As a company running an independent school only, First Bridge School does not qualify as a 'public authority'. This is affirmed by the definitions of 'public authority' and 'public body' given in both the Freedom of Information Act 2000 and the Data Protection Act 2018.

- As an educational provision, the 'core activity' at First Bridge School is therapeutic teaching, which does not inherently entail regular and systematic monitoring of data subjects on a 'large scale'.

- Neither the number of data subjects monitored nor the volume of personal data processed by First Bridge School qualifies as 'large scale' by a reasonable interpretation of the term, which remains undefined in statute.

So, for the purposes of centralising organisational responsibility, a data compliance officer has been designated. Ultimately, however, it remains the responsibility of the data controller (the company and school) to make final

decisions about whether to report a breach, disclose or amend a record or agree the terms of a contract with a data processor; the data compliance officer's role is one of advice and guidance.

The data compliance officer:

- monitors the organisation's compliance with the UK GDPR
- reports to the highest level of management (the CEO)
- will never be subject to dismissal, discipline or penalty for performing their duties.

Lawful processing

Under the UK GDPR, data will be lawfully processed when consent of the data subject has been obtained and processing is necessary for:

- compliance with a legal obligation
- the performance of a task carried out in the public interest
- the performance of a contract with the data subject or to take steps to enter into a contract
- protecting the vital interests of a data subject or another person.

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by law.

- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.

- Processing relates to personal data manifestly made public by the data subject.

- Carrying out obligations under employment.

- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.

- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.

Consent

- Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

- Where consent is given, a written record is kept, documenting how and when consent was given.

- First Bridge School ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease

- Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

- Consent can be withdrawn by the individual at any time.

- The consent of parents is sought prior to the processing of a child's data, with the exception of safeguarding concerns (legally required).

The Right to be Informed

- The privacy notice supplied to individuals in regard to the processing of their personal data is written in clear, plain language, which is concise, transparent, easily accessible and free of charge.

- Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

- Where data is not obtained directly from the data subject, information regarding the source the personal data originates from and whether it came from publicly accessible sources, will be provided.

- For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.

- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

The Right of Access

- Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

Information requests including Subject Access Requests (SARs)

- First Bridge Group Ltd will respond within one month to any written or emailed request for information which they hold or publish. Where a SAR has been made electronically, the information will be provided in an electronic format.

- The company will provide information on where to access the information required e.g. the website link, or details of a charge if the publication/ information is charged, or send any free information. If the item is charged the company does not need to provide it until the payment is received.

- A refusal of any information requested must state the relevant exemption which has been applied or that the company/school does

not hold the information, and must explain what public interest test has been made, if this applies.

- If the information is published by another organisation (for example, Ofsted or ISI reports) the company/school can direct the enquirer to the organisation which supplied the information or publication unless it is legal and possible to provide the information directly.

- It will not be legal to photocopy a publication in its entirety and supply this to an enquirer unless the company owns the copyright – this is particularly important where the original publication was a charged item.

- The company will keep the original request and note against this who dealt with the request and when the information was provided.

- Any complaint about the provision of information will be handled by the CEO. All complaints should be in writing and documented.

- All enquirers should be advised that they may complain to the Information Commissioner if they are unhappy with the way their request has been handled.

- Under the Freedom of Information Act a request for personal information can include unstructured as well as structured records – for example, letters, emails etc. not kept within an individual's personal files, or filed by their name, but still directly relevant to them. These can be requested if sufficient information is provided to identify them.

- Where a request is manifestly unfounded or excessive, First Bridge Group Ltd holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

SAR Procedure

- Requests for information must be made in writing; which includes email, and be addressed to the data compliance officer. If the initial request does not clearly identify the information required, then further enquiries will be made.

- The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child (if the information requested relates to a pupil). Evidence of identity can be established by requesting production of credible ID documents such as passport, birth certificate, P45/P46, bank statements with the current address, etc.

- The company may make a reasonable administration charge for the provision of information. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.

- The response time for subject access requests, once officially received, is one month. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

- In the event that a large quantity of information is being processed about an individual, we will ask the individual to specify the information the request is in relation to.

- All information will be reviewed prior to disclosure.

- Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information, consent should normally be obtained.

- Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.
- If there are concerns over the disclosure of information then additional advice should be sought.
- Where redaction has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

- Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

- Information can be provided on-site at First Bridge School with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then 'special delivery' mail must be used.

- Where an information request is made in relation to information held on a person other than yourself or your child, information will not be provided unless full written consent has been given by the person or persons whose information is being requested. However, even before requesting this written consent, advice will be sought from the Information Commissioner's Office (ICO).

- Subject access requests might, in the case of an employee file request for example, contain information identifying managers or colleagues who have contributed to (or are discussed in) that file. This may lead to a conflict between the requesting employee's right of access and the third party's rights over their own personal information. To decide whether to disclose information relating to a third-party individual, we follow ICO guidance. Whatever the decision, we will always keep a record of our course of action and the reasoning for it.

The Right to Rectification

- Individuals are entitled to have any inaccurate or incomplete personal data rectified.

- Where the personal data in question has been disclosed to third parties, we will inform them of the rectification where possible.

- Where appropriate, First Bridge Group Ltd will inform the individual about the third parties that the data has been disclosed to.

- Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

- Where no action is being taken in response to a request for rectification, we will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The Right to Erasure

- Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

1. Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
2. When the individual withdraws their consent.
3. When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
4. The personal data was unlawfully processed.
5. The personal data is required to be erased in order to comply with a legal obligation.
6. The personal data is processed in relation to the offer of information society services to a child.

First Bridge Group Ltd has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest.
- The exercise or defence of legal claims.
- As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

- Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

- Where personal data has been made public within an online environment, we will inform other organisations who process the

personal data to erase links to and copies of the personal data in question.

The Right to Restrict Processing

- Individuals have the right to block or suppress the processing of personal data.

- In the event that processing is restricted, we will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

First Bridge Group Ltd will restrict the processing of personal data in the following circumstances:

1. Where an individual contests the accuracy of the personal data, processing will be restricted until we have verified the accuracy of the data.

2. Where an individual has objected to the processing and we are considering whether their legitimate grounds override those of the individual.

3. Where processing is unlawful and the individual opposes erasure and requests restriction instead.

4. Where we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

5. If the personal data in question has been disclosed to third parties, we will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

6. We will inform individuals when a restriction on processing has been lifted.

The Right to Portability

- Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller.
- Where the processing is based on the individual's consent or for the performance of a contract.

And the following apply:

- When processing is carried out by automated means, personal data will be provided in a structured, commonly used and machine-readable form.
- We provide the information free of charge.
- Where feasible, data will be transmitted directly to another organisation at the request of the individual.
- We are not required to adopt or maintain processing systems which are technically compatible with other organisations.
- In the event that the personal data concerns more than one individual, we will consider whether providing the information would prejudice the rights of any other individual.
- We respond to any requests for portability within one month.
- Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.
- Where no action is being taken in response to a request, we will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The Right to Object

First Bridge Group Ltd will inform individuals of their right to object at the first point of communication, and this information will be outlined in the

privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

1. Processing based on legitimate interests or the performance of a task in the public interest
2. Direct marketing
3. Processing for purposes of research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests, an individual's grounds for objecting must relate to his or her particular situation.

First Bridge Group Ltd will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the organisation can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes we cannot refuse an individual's objection and will stop processing personal data for direct marketing purposes as soon as the objection is received.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.

- Where the processing of personal data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing of the data.

- Where the processing activity is outlined above, but is carried out online, we will offer a method for individuals to object online.

Privacy

First Bridge Group Ltd will act in accordance with the UK GDPR by adopting a privacy by design approach and implementing technical and organisational

measures which demonstrate how the organisation has considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the organisation's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to First Bridge Group Ltd.'s reputation which might otherwise occur.

A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large-scale processing of special categories of data or personal data which is in relation to criminal convictions or offences.

First Bridge Group Ltd will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk.

Where a DPIA indicates high risk data processing, we will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

Data Breaches

The term 'data breach' or 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The data compliance officer at First Bridge School will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of First Bridge Group Ltd becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, First Bridge Group Ltd will notify those concerned directly.

A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

In the event that a breach is sufficiently serious, First Bridge Group Ltd.'s stakeholders will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at First Bridge Group Ltd, which facilitate decision-making in relation to whether the relevant supervisory authority and/or the public need to be notified.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the data compliance officer
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects.

Data Security

- Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access.

- Confidential paper records are not left unattended or in clear view anywhere with general access.

- The data that is stored on our cloud servers is encrypted and 2FA protected. We do not have physical servers.

- Where data is saved on removable storage or a portable device, the device is kept in a locked filing cabinet, drawer or safe when not in use.

- Memory sticks are not used to hold personal information.

- All electronic devices are at least password-protected to protect the information on the device in case of theft.

- First Bridge Group Ltd commissions ITA to enable electronic devices to allow the remote blocking or deletion of data in case of theft.

- Staff are advised to not use their personal laptops or computers for work purposes.

- All necessary members of staff are provided with their own secure login and password. Any users with access to sensitive material held within Microsoft SharePoint have two-factor authentication enforced for their account, ensuring that even if their password is compromised the data to which they have access is still inaccessible to any would-be intruder.

- Documents attached to emails with sensitive or confidential information are password-protected.

- First Bridge School only emails parents occasionally, usually only in response to an email from a parent, if a parent has specifically requested to be emailed or if other means of communication have failed.

- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the organisation’s premises accepts full responsibility for the security of the data.

Before sharing data, all staff members must ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of First Bridge School containing sensitive information are supervised at all times.

The physical security of the organisation's school building and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

First Bridge Group Ltd takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action. The school ensures that continuity and recovery measures are in place to ensure the security of protected data.

Publication of Information

First Bridge Group Ltd only publicly publishes information about First Bridge School, such as prospectus information, policies and procedures. We will not publish any personal information, including photographs, on our website or on social-media channels without the permission of the affected individual. When uploading information to the school's website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

Photography and CCTV

- We will always indicate our intentions for taking photographs of pupils and always retrieve permission before publishing them. If First Bridge Group Ltd wishes to use images/video footage of pupils in a publication, such as the school's website, written permission is sought for the particular usage from the parent of the pupil.

- Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the UK GDPR.

- First Bridge Group Ltd makes no use of CCTV.

Software

First Bridge Group Ltd and First Bridge School use a range of market-leading software to fulfil its functions. These are subject to data protection impact assessments (DPIAs).

Data Retention

- Data will not be kept for longer than is necessary; unrequired data is deleted as soon as practicable.

- Some educational records relating to former pupils or employees of First Bridge Group Ltd may be retained for an extended period for legal reasons, but also to enable the provision of references.

- Paper documents will be shredded, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

DBS Data

- All data provided by the Disclosure & Barring Service (DBS) will be handled in line with data protection legislation; this includes electronic communication.

- Data provided by the DBS will never be duplicated.

- Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

Phonecalls

- Phonecalls at First Bridge School are recorded for monitoring and training purposes. All phonecalls, including internal calls, are recorded. They are securely retained in the 'cloud' for 30 days unless manually deleted. The only people with access to the recordings are ITA (our external IT consultants) on a strictly 'need to know' basis: for example, to investigate an allegation or an abusive phonecall. All phonecalls to First Bridge School includes the message "please note that we record all of our calls and by continuing this call you confirm acceptance of this" before the caller is put through to speak to somebody.

Confidentiality

- Employees are required to keep confidential about First Bridge Group Ltd.'s business and that of its pupils and families both during their employment and at any time after its termination.

- All information gained in the course of an employee's employment, remains confidential except in circumstances in which they are required to disclose information. Employees must not remove any documents or tangible items which belong to First Bridge Group Ltd or which contain any confidential information from the school's premises at any time without due cause. This includes the unauthorised use of any headed paper containing the school's logo and/or contact details.

- Employees must return to the schools if requested and, after consultation, and in any event upon the termination of your employment, all documents and tangible items which belong to First Bridge Group Ltd or which contain or refer to any confidential information and which are in their possession or under their control.

- Employees must, if requested by any leader, and after consultation, delete all confidential information from any re-usable material and destroy all other documents and tangible items which contain or refer to any confidential information and which are in their possession or under their control.

- Employees are not permitted to disclose information reproducing the company's or school's passwords or security codes to unauthorised personnel during their employment or at any time after termination of employment. Keys allocated by the school must not be passed on or made available to unauthorised persons within or external to the school.

- Employees who have access to the company's accounts and financial transactions are not permitted to disclose this information without the authorisation of the CEO.

Retention Periods

Pupils

Pupils' records (including CP/safeguarding files) will always be forwarded securely to their new school when they leave First Bridge School. Only the most basic administrative data will be retained, such as that required to fulfil the Education (Pupil Registration) (England) Regulations 2006, as well as any information required to fulfil clinical requirements as part of pupils' ABA programmes.

Staff

All personnel records (employees' 'staff files') are stored electronically on BreatheHR.

- Where there has been a CP/safeguarding allegation made against a member of staff, First Bridge School will retain their personnel records for 10 years or until the employee reaches retirement age, whichever is the longer.

- A member of staff's email account will be kept for three months (staff) or six months (leaders, aside from the DSL whose email account will be kept for one year) after their departure, unless involved in a safeguarding allegation that led to police action in which case they must be kept indefinitely.

- Any records that could be called as evidence in legal proceedings e.g. records relating to child sexual abuse concerns/disclosures or allegations against staff,
  must be kept indefinitely.

If none of the above apply, staff files will be retained for 6 years after the employee has left the employment of First Bridge Group Ltd.

All digital files that are retained in accordance with the conditions outlined above are securely and permanently deleted upon the expiration of their retention period.