Name of Policy:	Data Protection Policy
Author:	Katie Findlater
Applicable to:	Staff (including Employees, Governors, Trustees, and Volunteers), Students, Parents and Third Parties
Effective date:	28/10/2026
Date of next review:	27/10/2027

Version History Log

Version	Description of Change	Date of Policy Release
1.0	Original BRIT School Data Protection Policy.	17/01/2025
2.0	Updated to align with Judicium Master Template v15 (Data (Use and Access) Act 2025 updates, updated DPO contact details, lawful bases, international transfer rules, automated decision-making section, SAR clarification/search additions, and addition of SAR & Complaints Appendices).	28/10/2026

The BRIT School Commitment

The BRIT School is committed to providing a safe and secure environment for children, staff and visitors and promoting a climate where children and adults will feel confident about sharing any concerns which they may have about their own safety or the well being of others.

Aims

The BRIT School aims to ensure that all personal data collected about staff, pupils, parents, governors, 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 and amended by the Data (Use and Access) Act 2025.

Data Protection Act 2018 (DPA 2018).

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR.

- It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.
- In addition, 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.
- In addition, this policy complies with our funding agreement and articles of association.

Introduction

The UK General Data Protection Regulation (UK GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The School will protect and maintain a balance between data protection rights in accordance with the UK GDPR. This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, workers, governors, trustees, volunteers and other third parties.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Staff is defined by employees, governors, trustees and volunteers. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

The School is registered with the Information Commissioner's Office (ICO) as required Z646982X.

SECTION 1 – DEFINITIONS

Personal Data

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for example a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.
Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.
Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

Special Category Data and Data Relating to Criminal Convictions and Offences

Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical and mental health, sexuality and biometric or genetic data.

Personal data relating to criminal offences and convictions is included here for the

purposes of this policy. This refers to personal information relating to criminal convictions and offences, allegations, proceedings and related security measures.

Data Subject

An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.

Data Controller

The organisation storing and controlling such information (i.e. The BRIT School) is referred to as the Data Controller.

Processing

Processing data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Automated Processing

Any form of automated processing of personal data consists of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Examples of automated processing include profiling and automated decision-making. Automated decision-making is when a decision is made which is based solely on automated processing (without meaningful human intervention).

Data Protection Impact Assessment (DPIA)

DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Pseudonymised

The process by which personal data is processed in such a way that it cannot be used to identify an individual without the use of additional data, which is kept separately and subject to technical and organisational measures to ensure that the personal data

cannot be attributed to an identifiable individual.

SECTION 2 – WHEN CAN THE SCHOOL PROCESS PERSONAL DATA

Data Protection Principles

The BRIT School is responsible for and adheres to the principles relating to the processing of personal data as set out in the UK GDPR. The principles the BRIT School must adhere to are set out below.

Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner

The BRIT School only collects, processes and shares personal data fairly and lawfully and for specified purposes. The School must have a specified purpose for processing personal data and special category data as set out in the UK GDPR.

Before the processing starts for the first time, we will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues in order to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).

Personal Data

The School may only process a data subject's personal data if one of the following lawful bases are met:

- The data subject has given their consent;
- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- To perform a task in the public interest or in order to carry out official functions as authorised by law;
- For the purposes of the School's legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject;
- The processing is necessary for a recognised legitimate interest under the UK GDPR (as amended by the Data (Use and Access) Act 2025).

Special Category Data

The School may only process special category data if they are entitled to process personal data (using one of the lawful bases above) AND one of the following conditions are met:

- The data subject has given their explicit consent;

- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the School in the field of employment law, social security law, or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private healthcare insurance, and providing contractual sick pay;
- To protect the data subject's (or another person's) vital interests, where the data subject is unable to give consent;
- The processing is necessary for the establishment, exercise, or defence of legal claims or whenever courts are acting in their judicial capacity;
- Where the data has been made public by the data subject;
- To perform a task in the substantial public interest or in order to carry out official functions as authorised by law;
- Where it 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, or the management of health or social care systems and services;
- Where it is necessary for reasons of public interest in the area of public health;
- The processing is necessary for archiving, statistical, or research purposes.

The School identifies and documents the legal grounds being relied upon for each processing activity.

Criminal Record Data

Where criminal records data is processed, a lawful condition for processing that data is also identified and documented.

Consent

Where the School relies on consent as a lawful basis for processing (as set out above), it will adhere to the requirements set out in the UK GDPR.

Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent is needed in cases of processing special category data and requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

A data subject will have consented to processing of their non-special category personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

In cases of processing special category data and explicit consent, the School will

normally seek another legal basis to process that data. However, if explicit consent is required, the data subject will be provided with full information in order to provide explicit consent.

The School will keep records of consents obtained in order to demonstrate compliance with consent requirements under the UK GDPR.

Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes

Personal data will not be processed in any manner that is incompatible with the legitimate purposes specified.

The School will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purpose (and they have consented where necessary).

Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

The School will only process personal data when our obligations and duties require us to. We will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes.

When personal data is no longer needed for specified purposes, the School shall delete or anonymise the data. Please refer to The BRIT School's Data Retention Policy for further guidance.

Principle 4: Personal data must be accurate and, where necessary, kept up to date

The School will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the School.

Principle 5: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed

Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The School will ensure that they adhere to legal timeframes for retaining data.

We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices.

Please refer to the School's Data Retention Policy for further details about how the School retains and removes data.

Principle 6: Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage

In order to ensure the protection of all data being processed, the School will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as:

- Encryption;
- Pseudonymisation (as outlined above);
- Ensuring authorised access on both hard copy and electronic files (i.e. that only people who have a need to know the personal data are authorised to access it);
- Adhering to confidentiality principles;
- Ensuring personal data is accurate and suitable for the process for which it is processed.

The School follows procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.

The School will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place. Full details on the School's security measures are set out in the School's Information Security Policy.

Sharing Personal Data

The School will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. The following points will be considered:

- Whether the third party has a need to know the information for the purposes of providing the contracted services;
- Whether sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;

- Whether the third party has agreed to comply with the required data security standards, policies, and procedures and implemented adequate security measures;
- Whether the transfer complies with any applicable cross-border transfer restrictions; and
- Whether a fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

There may be circumstances where the School is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities, for example, the Local Authority, Ofsted or the Department of Health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of our School shall be clearly defined within written notifications including details and the basis for sharing that data.

Transfer of Data Outside the UK

The UK GDPR restricts the transfer of personal data to countries or international organisations outside of the UK to ensure that individuals' data continues to receive an adequate level of protection.

The School will not transfer personal data outside of the UK unless:

- The destination country is covered by a UK adequacy regulation;
- Appropriate safeguards are in place, such as a UK International Data Transfer Agreement (IDTA) or an approved set of standard contractual clauses, and enforceable data subject rights and effective legal remedies are available;
- A specific derogation applies under Article 49 UK GDPR (for example, the transfer is necessary for an important reason of public interest).

All staff must comply with the School's guidelines on transferring personal data outside of the UK. For clarity, a "transfer" may occur whenever personal data are sent, accessed, viewed or otherwise made available from outside the UK.

The School monitors any international transfers with support from the Data Protection Officer (DPO) and maintains records of our transfer assessments alongside a Third-Party Data Sharing Register.

SECTION 3 – DATA SUBJECT'S RIGHTS AND REQUESTS

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.

The rights data subjects have in relation to how the School handles their personal data are set out below:

- (Where consent is relied upon as a condition of processing) To withdraw consent to processing at any time;
- Receive certain information about the School's processing activities;
- Request access to their personal data that we hold (see "Subject Access Requests" at Appendix 1);
- Prevent our use of their personal data for direct marketing purposes;
- Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
- Restrict processing in specific circumstances, such as where the accuracy of the data is contested or an objection is being considered;
- Challenge processing which has been justified on the basis of legitimate interests or in the public interest;
- Request a copy of an agreement under which personal data is transferred outside of the UK;
- To be informed where a decision that has legal or similarly significant effects is made solely by automated means, and to request human intervention, express their point of view, or contest a decision;
- Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
- To raise a concern or make a complaint directly to the School if they believe their personal data has been processed unlawfully or unfairly, or if they are dissatisfied with the School's response to a data protection request. Individuals also have the right to make a complaint to the supervisory authority, which is the Information Commissioner's Office (ICO); and
- In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the School to verify the identity of the individual making the request.

Direct Marketing

The School is subject to certain rules and privacy laws when marketing. For example, a data subject's prior consent will be required for electronic direct marketing (for example, by email, text or automated calls).

The School will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The School will promptly respond to any individual objection to direct marketing.

Employee Obligations

Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the School in the course of their employment or engagement. If so, the School expects those employees to help meet the School's data protection obligations to those individuals. Specifically, you must:

- Only access the personal data that you have authority to access and only for authorised purposes;
- Only allow others to access personal data if they have appropriate authorisation;
- Keep personal data secure (for example by complying with rules on access to school premises, computer access, password protection and secure file storage and destruction. Please refer to the School's Information Security Policy for further details about our security processes);
- Not remove personal data or devices containing personal data from the School premises unless appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information;
- Not store personal information on local drives.

SECTION 4 – ACCOUNTABILITY

The School will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the UK GDPR principles.

The School has taken the following steps to ensure and document UK GDPR compliance:

Data Protection Officer (DPO)

Please find below details of the School's Data Protection Officer:

Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 (option 1, then option 1 again)
Lead Contact: Craig Stilwell

The DPO is responsible for overseeing this Data Protection Policy and developing data-related policies and guidelines.

Should staff have any questions about the UK GDPR, the operation of this policy, or if you have any concerns that this policy is not being or has not been followed, please contact Katie Findlater in the first instance. Should the matter remain unresolved or require further escalation, please contact the School's DPO.

In particular, you can contact the DPO in the following circumstances:

- If you are unsure of the lawful basis being relied on by the School to process personal data;
- If you need to rely on consent as a lawful basis for processing;
- If you need to draft privacy notices or policies;
- If you are unsure about the retention periods for the personal data being processed;
- If you are unsure about what security measures need to be put in place to protect personal data;
- If there has been a personal data breach;
- If you are unsure on what basis to transfer personal data outside the UK;
- If you need any assistance dealing with any rights invoked by a data subject;
- Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;
- If you plan to undertake any activities involving automated processing or automated decision-making;
- If you need help complying with applicable law when carrying out direct marketing activities;
- If you need help with any contracts, data processing agreements, or other areas in relation to sharing personal data with third parties.

Data Subject Complaints

Individuals have the right to make a complaint directly to us if they believe their data protection rights have been breached.

We will acknowledge receipt within 30 days and provide a substantive response without undue delay. If you are not satisfied with our response, you may escalate the matter to the Information Commissioner's Office (ICO).

Further information about how the School handles data protection complaints can be found at Appendix 3 of this policy, along with a data protection complaints form at Appendix 4. Complaints can be made in writing to dpo-brit@brit.croydon.sch.uk.

Personal Data Breaches

The UK GDPR requires the School to notify any applicable personal data breach to the Information Commissioner's Office (ICO).

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so. Please refer to our Data Breach Policy.

If you know or suspect that a personal data breach has occurred, do not attempt to

investigate the matter yourself. Immediately contact the person designated as the key point of contact for personal data breaches (who is Katie Findlater) or the School DPO.

Transparency and Privacy Notices

The School will provide detailed, specific information to data subjects. This information will be provided through the School's privacy notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. The School's privacy notices are tailored to suit the data subject and set out information about how the School uses their data.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the UK GDPR. This includes the identity of the Data Protection Officer, the School's contact details, how and why we will use, process, disclose, protect and retain personal data. This information will be provided within our privacy notices.

When personal data is collected indirectly (for example, from a third party or a publicly available source), where appropriate, we will provide the data subject with the above information as soon as possible after receiving the data. The School will also confirm whether that third party has collected and processed data in accordance with the UK GDPR.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as "children" under the UK GDPR.

Privacy by Design

The School adopts a privacy-by-design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the School takes into account the nature and purposes of the processing, any cost of implementation and any risks to the rights and freedoms of data subjects when implementing data processes.

Data Protection Impact Assessments (DPIAs)

In order to achieve a privacy-by-design approach, the School conducts DPIAs for any new high-risk technologies or programmes being used by the School which could affect the processing of personal data. The School carries out DPIAs when required by the UK GDPR in the following circumstances:

- For the use of new technologies (programs, systems or processes) or changing technologies;

- For the use of automated processing;
- For large scale processing of special category data; and
- For large-scale, systematic monitoring of a publicly accessible area (for example, through the use of CCTV).

Our DPIAs contain:

- A description of the processing, its purposes and any legitimate interests used;
- Details of what types of data are shared;
- Steps taken by the third party and the school in order to protect data;
- An assessment of the necessity and proportionality of the processing in relation to its purpose;
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.

Record Keeping

The School is required to keep full and accurate records of our data processing activities (Records of Processing Activities (ROPA)). These records include:

- The name and contact details of the School;
- The name and contact details of the Data Protection Officer;
- Descriptions of the types of personal data used;
- Description of the data subjects;
- Details of the School's processing activities and purposes;
- Details of any third party recipients of the personal data;
- Where personal data is stored;
- Retention periods; and
- Security measures in place.

Training

The School will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws. The School will carry out adequate training with all staff as part of induction and as regular refreshers.

Audit

The School, through its Data Protection Officer (Judicium), regularly tests our data systems and processes in order to assess compliance. These are done through data audits which take place annually in order to review use of personal data.

Related Policies

Staff should refer to the following policies that are related to this Data Protection Policy:

1. Data Protection Policy (inclusive of SAR & Complaints appendices);
2. Data Breach Policy;

3. Data Retention Policy;
4. Freedom of Information Policy and Publication Scheme;
5. Acceptable Use Policy;
6. CCTV Policy (if used);
7. IT Security / Cyber Security Policy.
8.

These policies are also designed to protect personal data and can be found on the School portal.

Monitoring

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate. Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the School.

SECTION 5 – AUTOMATED PROCESSING AND AUTOMATED DECISION MAKING

Automated decision making takes place when an electronic system uses personal information to make a decision without human intervention. We are required to ensure that appropriate safeguards are in place when using automated decision making for significant decisions and the circumstances in which we are permitted to use special category data (sensitive information) in automated decision making are limited.

You will not be subject to automated decision making for significant decisions unless we have a lawful basis for doing so, including a valid condition where required and appropriate safeguards are in place. Appropriate safeguards include informing the relevant individuals about the automated decision making and their rights to request a human review, express their views, and contest the decision.

The School will carry out a Data Protection Impact Assessment before any new automated processing or automated decision-making activities are undertaken.

APPENDIX 1 – SUBJECT ACCESS REQUESTS

Under Data Protection Law, Data Subjects have a general right to find out whether the School holds or processes personal data about them, to access that data and to be given supplementary information. This is known as the right of access or the right to make a data subject access request (SAR).

The purpose of the right is to enable the individual to be aware of and verify the lawfulness of the processing of personal data that the School is undertaking. It is designed to assist individuals in understanding how and why we are using their data and to check that we are doing so lawfully. The main provisions are to be found in Articles 12 and 15 of the UK GDPR and Section 45 of the Data Protection Act 2018. This appendix provides guidance for staff members on how data subject access requests should be handled and for all individuals on how to make a SAR.

Failure to comply with the right of access under UK GDPR puts both staff and the School at potentially significant risk and so the School takes compliance with this policy very seriously.

A Data Subject has the right to be informed by the School of the following:

- Confirmation that their personal data is being processed;
- Access to their personal data;
- The following 'supplementary information':
    - The purposes of processing;
    - The categories of personal data concerned;
    - The recipients or categories of recipients to whom the data have been or will be disclosed;
    - Where possible, the period for which the data will be stored or the criteria used to determine that period;
    - The existence of the data subject's rights to rectification, erasure, restriction, objection and data portability;
    - The right to lodge a complaint with the ICO;
    - Where the data were not collected directly from the individual, any available information about the source;
    - Any automated decision-making, including profiling and information about the logic involved, as well as the significance and envisaged consequences of such processing; and
    - Where relevant, details of the safeguards applied to data transferred outside the UK.

Dealing with a SAR is time critical and must be prioritised. Other than in exceptional cases, we will have only one month in which to respond to a SAR and even if an extension of the time limit is permitted, the individual must still be informed within that month of the fact that the request will take longer to process and the reasons for the delay. Failure to deal with a SAR within that period could leave us open to the possibility of being fined by the ICO.

All staff must be aware of the potential for receiving a SAR and the importance of dealing with such a request as a matter of urgency. Anyone within the School may receive a SAR. It does not need to be made to a nominated person. It will be equally as valid if sent to anyone within the school. A SAR does not need to be in writing and can be made verbally, by post, by email, WhatsApp text or social media where relevant.

How to Recognise a Subject Access Request

A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g. a solicitor or a parent making a request in relation to information relating to their child):

- For confirmation as to whether the School processes personal data about him or her and, if so
- For access to that personal data
- And/or certain other supplementary information (listed above).

A data subject is generally only entitled to access their own personal data and not information relating to other people.

How to Make a Data Subject Access Request

While there is no requirement to do so, we encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data being requested. If a request is made verbally, we will ensure we follow this up with something in writing to confirm what has been requested and outline the timeframe for dealing with the request.

What to do When You Receive a Data Subject Access Request

All data subject access requests should be immediately directed to Katie Findlater, who should contact Judicium as DPO in order to assist with the request.

Acknowledging the Request

When receiving a SAR the School shall acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request.

Verifying Identity and Requesting Clarification

Before responding to a SAR, the School will take reasonable steps to verify the identity of the person making the request. When it is necessary to verify identity, the one calendar month period for responding begins when sufficient confirmation of identity is provided.

When it is necessary to request more information for the purpose of clarifying the

request, the one calendar month period for responding may be paused when further information is requested and does not restart until sufficient clarification is provided.

Requests Made by Third Parties or on Behalf of Children

The school needs to be satisfied that the third party making the request is entitled to act on behalf of the individual. Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, the School will usually require the written authorisation of the child before responding to the requester or providing the personal data directly to the child.

Fee for Responding to a SAR

The School will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive, a reasonable fee to cover administrative costs may be requested. If a fee is requested, the period of responding begins when the fee has been received.

Time Period for Responding to a SAR

The School has one calendar month to respond to a SAR. If the deadline falls on a weekend or public holiday, the deadline will be the next working day. The period for response may be extended by a further two calendar months in relation to complex requests.

School Closure Periods

Requests received during or just before school closure periods may not be able to be responded to within the one calendar month response period because the School may be closed or have limited staff on site. The School will endeavour to comply with requests as soon as possible upon re-opening.

Information to be Provided & Format

Where a request is made by electronic means, and unless the requestor asks otherwise, the School will normally provide the information in a commonly used electronic format (for example, PDF).

How to Locate Information

Depending on the type of information requested, the School may need to search all or some of the following:

- Electronic systems (databases, computers, servers, email, backup data, CCTV);
- Manual filing systems;
- Data systems held externally by data processors;
- Safeguarding systems (such as CPOMS, MyConcern);
- MIS systems (such as SIMS, Bromcom, Arbor);

- Occupational health records, pensions data, insurance benefit information.

We will handle data subject rights requests and searches in a manner that is reasonable and proportionate to the nature of the request, the amount of data involved and the effort required. We will not conduct searches that would impose a disproportionate burden on our operations.

Exemptions & Protection of Third Parties

The School does not have to disclose personal data that identifies another individual unless that individual consents or it is reasonable to comply without consent. Other exemptions include crime detection/prevention, confidential references (given or received), legal professional privilege, management forecasting and negotiations.

Refusing to Respond to a Request

The school can refuse to comply with a SAR if it is manifestly unfounded or excessive, or to avoid obstructing legal inquiries/investigations. In such cases, the data subject must be informed within one month of the reasons for refusal and their right to complain to the ICO.

APPENDIX 2 – SUBJECT ACCESS REQUEST FORM

Please complete this form if you wish to make a request for your personal data held by The BRIT School.

Section 1 – Data Subject Details

Title:	
Surname/Family Name:	
First Name(s):	
Date of Birth:	
Address:	
Postcode:	
Phone Number:	
Email Address:	

Enclosed Proof of Identity:
☐ Birth Certificate ☐ Driving Licence ☐ Passport ☐ Official Utility Letter

Section 2 – Representative Details (if applicable)

If you are applying on behalf of the data subject, please complete your details below and provide proof of authorisation.

Title:	
Surname/Family Name:	
First Name(s):	
Relationship to Data Subject:	
Address & Contact Info:	

Proof of Authorisation Enclosed:
☐ Letter of Authority ☐ Power of Attorney ☐ Evidence of Parental Responsibility

Section 3 – Data Requested

Please describe in as much detail as possible what data you request access to (e.g. date range, specific correspondence, student/staff records):

Preferred Format:
☐ Email (Electronic PDF) ☐ Post ☐ View in Person

Please send the completed form to: dpo-brit@brit.croydon.sch.uk

APPENDIX 3 – DATA PROTECTION COMPLAINTS

Under Data Protection Law, individuals have the right to raise concerns or make complaints about the way their personal data has been handled by the School.

What is a Data Protection Complaint?

A data protection complaint is any expression of dissatisfaction from an individual regarding how the School has processed their data or handled a data protection request (e.g., inaccurate data, unlawful processing, SAR delay, security breach).

How to Make a Complaint

Complaints can be made verbally or in writing. Complainants are encouraged to use Appendix 4 (Data Protection Complaints Form) and submit it to dpo-brit@brit.croydon.sch.uk

Acknowledging and Investigating

The School will acknowledge receipt within 30 days and provide a substantive response as soon as reasonably practicable. All complaints will be investigated promptly and confidentially in consultation with the DPO.

Outcome & Escalation

Following investigation, the School will issue a written response explaining findings and corrective actions. If dissatisfied, the complainant has the right to escalate the matter to the Information Commissioner's Office (ICO).

APPENDIX 4 – DATA PROTECTION COMPLAINTS FORM

Please complete this form to submit a formal data protection complaint to The BRIT School.

Section 1 – Complainant Details

Full Name:	
Contact Phone / Email:	
Address:	

Section 2 – Complaint Details

Please describe your concern in detail (including dates, names and any relevant background):

Have you previously raised this concern with the School? ☐ Yes ☐ No

What outcome are you seeking?

Section 3 – Declaration

☐ I confirm that the information provided is accurate to the best of my knowledge.

Signature: _____ Date: _____