Data Protection Policy

Full School including EYFS

2026/2027

Ibstock Place

CO-EDUCATIONAL DAY SCHOOL

IBSTOCK PLACE SCHOOL

Data Protection Policy

Full School including EYFS

Scope

This policy applies to all pupils (aged 4 (EYFS) – 18) and staff at Ibstock Place School (hereinafter 'Ibstock' or 'the School').

Roles and Responsibilities

The Governing Body has a statutory responsibility to ensure that this policy is ratified and compliant, as set out in the Independent School Standards 2019 (ISS). The Governing Body delegates this responsibility to the Head, who is accountable for the operationalisation of this policy. In turn, the Bursar is delegated responsibility for the consistent application and implementation of this statutory policy across the School. Staff must follow the expectations set out in this policy.

1. 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 are obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

Ibstock 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 and other third parties.

This policy does not form part of any individual's terms and conditions of employment with Ibstock 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. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action up to and including summary dismissal depending on the seriousness of the breach.

2. 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.

Special Category Data

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 or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

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., Ibstock) 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 organisation, 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 consisting 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.

An example of automated processing includes profiling and automated decision-making. Automated decision-making is when a decision is made which is based solely on automated processing (without human intervention) which produces legal effects or significantly affects an individual. Automated decision-making is prohibited except in exceptional circumstances.

Data Protection Impact Assessment (DPIA)

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

Criminal Records Information

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

3. When can Ibstock process Personal Data?

Data Protection Principles

Ibstock 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 School must adhere to are set out below.

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

Ibstock only collects, processes and shares personal data fairly and lawfully and for specified purposes. Ibstock 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 shall 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

Ibstock may only process a data subject's personal data if one of the following fair processing conditions is 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.

Special Category Data

Ibstock may only process special category data if it is entitled to process personal data (using one of the fair processing conditions 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 Ibstock 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 health care insurance and providing contractual sick pay.
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- 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.

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

Consent

Where Ibstock relies on consent as a fair condition 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 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 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.

If explicit consent is required, Ibstock 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.

Ibstock 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.

Ibstock 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 shall 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, Ibstock Place will delete or anonymise the data. Please refer to the School's Data Retention Policy for further guidance.

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

Ibstock 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. Ibstock 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 Retention Policy for further details about how Ibstock 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 assure the protection of all data being processed, Ibstock will develop, implement and maintain reasonable safeguards and security measures. This includes using measures such as:

- Encryption

- Pseudonymisation (this is where Ibstock replaces information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure);
- Ensuring authorised access (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.

Ibstock 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.

Ibstock 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.

Sharing Personal Data

Ibstock will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. These include if the third party:

- Has a need to know the information for the purposes of providing the contracted services;
- 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;
- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- The transfer complies with any applicable cross border transfer restrictions; and
- A fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

There may be circumstances where Ibstock 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, Independent Schools Inspectorate 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 Ibstock will be clearly defined within written notifications and details and basis for sharing that data given.

Transfer of Data Outside the European Economic Area (EEA)

The UK GDPR restricts transfers of data to countries outside the UK and EEA in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined.

Ibstock will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the UK GDPR. All staff must comply with Ibstock's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

Transfer of Data Outside the UK

The School may transfer personal information outside the UK and/or to international organisations on the basis that the country, territory or organisation is designated as having an adequate level of protection or that the organisation receiving the information has provided adequate safeguards by way of binding corporate rules, standard data protection clauses or compliance with an approved code of conduct.

4. 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 that data subjects have in relation to how Ibstock handles its personal data are set out below:

(a) (Where consent is relied upon as a condition of processing) to withdraw consent to processing at any time

(b) Receive certain information about Ibstock's processing activities

(c) Request access to their personal data that we hold (see "Subject Access Requests" at Appendix 1)

(d) Prevent our use of their personal data for marketing purposes

(e) 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

(f) Restrict processing in specific circumstances

(g) Challenge processing which has been justified on the basis of our legitimate interests or in the public interest

(h) Request a copy of an agreement under which personal data is transferred outside of the UK + EEA

(i) Object to decisions based solely on automated processing

(j) Prevent processing that is likely to cause damage or distress to the data subject or anyone else

(k) Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms

(l) Make a complaint to the supervisory authority; and

(m) 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 Ibstock to verify the identity of the individual making the request.

Complaints Relating to Data Protection Handling and Data Subject Access Requests

Individuals may complain about:

- The collection, use, sharing or retention of personal data.
- Responses to Subject Access Requests.
- Perceived breaches of UK GDPR or the Data Protection Act 2018.
- Data security incidents affecting their personal information.

Complaints of this nature will be handled following the procedure outlined in the School's Complaints Policy.

Direct Marketing

Ibstock 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).

Ibstock 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. Ibstock 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 Ibstock in the course of their employment or engagement. If so, the School expects those employees to help meet Ibstock'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
- Not remove personal data or devices containing personal data from Ibstock's premises unless appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information
- Not to store personal information on local drives

5. Accountability

Ibstock 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.

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

Data Protection Officer (DPO)

Please find below details of Ibstock's Data Protection Officer:

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 020 3326 9174
Lead Contact: Craig Stilwell

The DPO is responsible for overseeing this data protection policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

(a) If you are unsure of the lawful basis being relied on by Ibstock to process personal data

(b) If you need to rely on consent as a fair reason for processing (please see below the section on consent for further detail)

(c) If you need to draft privacy notices or fair processing notices

(d) If you are unsure about the retention periods for the personal data being processed [but would refer you to the School's Data Retention Policy in the first instance]

(e) If you are unsure about what security measures need to be put in place to protect personal data

(f) If there has been a personal data breach [and would refer you to the procedure set out in the School's Data Breach policy]

(g) If you are unsure on what basis to transfer personal data outside the EEA

(h) If you need any assistance dealing with any rights invoked by a data subject

(i) 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 for what it was collected

(j) If you plan to undertake any activities involving automated processing or automated decision-making

(k) If you need help complying with applicable law when carrying out direct marketing activities

(l) If you need help with any contracts or other areas in relation to sharing personal data with third parties

Personal Data Breaches

The UK GDPR requires Ibstock 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.

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 the Ibstock Data Manager or your DPO.

Transparency and Privacy Notices

Ibstock will provide detailed, specific information to data subjects. This information will be provided through Ibstock'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. Privacy notices set out information for data subjects about how the School uses its data and the School's privacy notices are tailored to suit the data subject.

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 including the identity of the data protection officer, Ibstock's contact details, how and why we will use, process, disclose, protect and retain personal data. This will be provided in our privacy notice.

When personal data is collected indirectly (for example from a third party or publicly available source), we shall provide the data subject with the above information as soon as possible after receiving the data. Ibstock 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

Ibstock 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, Ibstock takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

Data Protection Impact Assessments (DPIAs)

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

- For the use of new technologies (programmes, systems or processes) or changing technologies
- For the use of automated processing
- For large scale processing of special category data
- For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV)

Our DPIAs contain:

- A description of the processing, its purposes and any legitimate interests used
- 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

Ibstock is required to keep full and accurate records of our data processing activities. 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
- Descriptions 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

Ibstock will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws.

Audit

Ibstock, through its Data Protection Officer, regularly tests our data systems and processes to assess compliance. These are carried out through data audits which take place regularly 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:

- Data Retention Policy

- Data Breach Policy

These policies are also designed to protect personal data and can be accessed by contacting the school.

Monitoring

We shall 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 Ibstock.

6. Automated Processing and Automated Decision-Making

Automated decision-making is generally prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) The data subject has given explicit consent

(b) The processing is authorised by law; or

(c) The processing is necessary for the performance of or entering into a contract

If certain types of sensitive data are being processed, then (b) or (c) above will not be allowed unless it is necessary for the substantial public interest (for example, fraud prevention).

If a decision is to be based solely on automated processing, then data subjects must be informed of their right to object. This right will be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the data subject's rights and freedoms and legitimate interests.

The School will also inform the data subject of the logic involved in the decision-making or profiling, the significance and envisaged consequences and give the data subject the right to request human intervention, express their point of view or challenge the decision.

The School will carry out a data protection impact assessment before any automated processing or automated decision-making activities are undertaken.

Queries

Queries on this policy should be directed to the Bursar.

Review and Verification

This policy is reviewed annually by the Bursar.

Appendix

Please see overleaf for Appendix 1.

Appendix 1 – Subject Access Requests

Under Data Protection Law, Data Subjects have a general right to find out whether Ibstock 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 Ibstock is undertaking.

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

(a) Confirmation that their data is being processed

(b) Access to their personal data

(c) A description of the information that is being processed

(d) The purpose for which the information is being processed

(e) The recipients/class of recipients to whom that information is or may be disclosed

(f) Details of Ibstock's sources of information

(g) In relation to any Personal Data processed for the purposes of evaluating matters in relation to the Data Subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision-making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct; and

(h) Other supplementary information

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

A valid SAR can be both in writing (by letter, email, WhatsApp message) or verbally (e.g. during a telephone conversation). The request may refer to the UK GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of information that Ibstock or the School holds about me' will be a data subject access request and should be treated as such.

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

Whilst 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. This allows Ibstock to easily recognise that you wish to make a data subject access request and the nature of your request. If the request is unclear/ vague we may be required to clarify the scope of the request which may in turn delay the start of the time period 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 the School's Data Manager who should contact Judicium as DPO in order to assist with the request and what is required.

Acknowledging the request

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

In addition to acknowledging the request, Ibstock may ask for:

- proof of ID (if needed)
- further clarification about the requested information
- if it is not clear where the information shall be sent, Ibstock must clarify what address/email address to use when sending the requested information; and/or
- consent (if requesting third party data)

Ibstock should work with its DPO in order to create the acknowledgment.

Verifying the identity of a requester or requesting clarification of the request

Before responding to a SAR, Ibstock will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward. Ibstock is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Where Ibstock has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of a passport, driving licence, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.

If an individual is requesting a large amount of data Ibstock may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be asked

why the request has been made. Ibstock shall let the requestor know as soon as possible where more information is needed before responding to the request.

In both cases, the period of responding begins when the additional information has been received. If Ibstock does not receive this information, they will be unable to comply with the request.

Requests made by third parties or on behalf of children

Ibstock needs to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney. Ibstock may also require proof of identity in certain circumstances.

When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else such as a parent or guardian, to have access to the child's personal data. Before responding to a SAR for information held about a child, Ibstock should consider whether the child is mature enough to understand their rights. If Ibstock is confident that the child can understand their rights, then the School should usually respond directly to the child or seek their consent before releasing their information.

It will be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- the child's level of maturity and their ability to make decisions like this
- the nature of the personal data
- any court orders relating to parental access or responsibility that may apply
- any duty of confidence owed to the child or young person
- any consequences of allowing those with parental responsibility access to the child's or young person's information; this is particularly important if there have been allegations of abuse or ill-treatment
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them

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, then provided that Ibstock is confident that they understand their rights, and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the School will require the written authorisation of the child before responding to the requester, or provide the personal data directly to the child.

Ibstock may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example if it is likely to cause detriment to the child.

Fee for responding to a SAR

Ibstock will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee to cover administrative costs may be requested.

The School may charge the requester a fee for providing the requested information. This will be dependent on whether the staffing costs in complying with the request exceed the threshold. The threshold is currently £450 with staff costs calculated at a fixed rate of £30 per hour (therefore 15 hours' work is required before the threshold is reached).

If a request would cost less than the threshold, then the school can only charge for the cost of informing the applicant whether the information is held, and communicating the information to the applicant (e.g. photocopying, printing and postage costs).

When calculating costs/threshold, the School can take account of the staff costs/time in determining whether the information is held by the School, locating and retrieving the information, and extracting the information from other documents. The School will not take account of the costs involved with considering whether information is exempt under the Act.

If a request would cost more than the appropriate limit, (£450) the school can turn the request down, answer and charge a fee or answer and waive the fee.

If the School are going to charge they will send the enquirer a fees notice. The School does not have to comply with the request until the fee has been paid. More details on fees can be found on the ICO website.

If planning to turn down a request for cost reasons, or charge a high fee, the School will contact the applicant in advance to discuss whether they would prefer the scope of the request to be modified so that, for example, it would cost less than the appropriate limit.

Where two or more requests are made to the School by different people who appear to be acting together or as part of a campaign the estimated cost of complying with any of the requests may be taken to be the estimated total cost of complying with them all.

Time Period for Responding to a SAR

Ibstock has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, Ibstock will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

Ibstock 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. This is because there may be no one on site to comply with the request. As a result, it is unlikely that your request will be able to be dealt with during this time. We may not be able to acknowledge your request during this time (i.e. until a time when we receive the request), however, if we can acknowledge the request, we may still not be able to deal with it until school reopens. Ibstock will endeavour to comply with requests as soon as possible and will keep in communication with you as far as possible. If your request is urgent, please provide your request during term times and not during/close to closure periods.

The School monitors and processes Subject Access Requests during normal working hours only. Requests received during weekends, bank holidays, public holidays or other periods when the School is closed will be logged and actioned on the first working day following receipt.

This administrative arrangement does not affect any statutory timescales applicable under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Information to be provided in response to a request

The individual is entitled to receive access to the personal data we process about him or her.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly-used electronic format.

The information that Ibstock is required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as Ibstock

has one month in which to respond, Ibstock is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR.

Ibstock is therefore, allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. Ibstock is not allowed to amend or delete data to avoid supplying the data.

How to locate information

The personal data Ibstock needs to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

Protection of third parties -exemptions to the right of subject access

There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case-by-case basis.

Ibstock will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then Ibstock does not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent

In determining whether it is reasonable to disclose the information without the individual's consent, all of the relevant circumstances will be taken into account, including:

- the type of information that they would disclose
- any duty of confidentiality they owe to the other individual
- any steps taken to seek consent from the other individual
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to Ibstock disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent,

Ibstock must decide whether to disclose the information anyway. If there are any concerns in this regard, then the DPO should be consulted.

Other exemptions to the right of subject access

In certain circumstances, Ibstock may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

Crime detection and prevention: Ibstock does not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any taxes or duties.

Confidential references: Ibstock does not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

- education, training or employment of the individual
- appointment of the individual to any office; or
- provision by the individual of any service

This exemption does not apply to confidential references that Ibstock receives from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e. the person giving the reference), which means that Ibstock must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

Legal professional privilege: Ibstock does not have to disclose any personal data which is subject to legal professional privilege.

Management forecasting: Ibstock does not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

Negotiations: Ibstock does not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

Vexatious Requests

There is no obligation on the School to comply with vexatious requests. A vexatious request is one which is designed to cause inconvenience, harassment or expense rather than to obtain information, and would require a substantial diversion of resources or would otherwise undermine the work of the school. However, this does not provide an excuse for bad records management.

In addition, the School does not have to comply with repeated identical or substantially similar requests from the same applicant unless a reasonable interval has elapsed between requests.