



General Data Protection Regulation (GDPR)

Adopted by Governors: Autumn 2018
Union Meeting (if applicable) NA

Next Review due: Spring 2027

Committee Reviewed at: ...Full – Spring 2026

Signed by Chair of Committee:
Date 20/03/2026

Signed by Head Teacher:
Date: 20/03/2026

Data Protection Statement

Birkett House School is committed to working effectively to provide a secure environment to protect data that it holds and stores. Whilst there is a statutory duty that is important, the fact that the School stores data about individuals means that it is responsible for data about students and that is taken seriously. This policy, and the Privacy Notices, sets out how we look after and use data.

The school will be responsible for the day-to-day management of data that is held about pupils, staff, parents, carers and other individuals in connection with that school.

GDPR policy builds trust and helps staff and parents understand the school's data protection practices, reducing the risk of misunderstandings or complaints. It acts as a safeguard in the event of regulatory audits or inquiries by the Information Commissioner's Office (ICO).

The School collects and process personal data to fulfil its educational, legal, and administrative obligations, ensuring data is handled lawfully, fairly, and transparently. All personal information is securely stored, and the school implements robust measures to safeguard it against unauthorized access or loss.

Data may be shared with third parties such as local authorities, examination boards, or healthcare providers, only when necessary and in compliance with legal requirement

What is the General Data Protection Regulation (UK GDPR)?

This is a European Directive that was brought into UK law with an updated Data Protection Act (DPA) for May 2018. It was brought into line with changes to the UK leaving the EU on 31 December 2020.

The GDPR and new DPA exist to look after individual's data. It is a series of safeguards for every individual. Information about individuals needs to be treated with respect and be secure. The GDPR exists to protect individual rights in an increasingly digital world.

Who does it apply to?

Everyone, including schools. As Public Bodies schools have more obligations than some small businesses. It is mandatory to comply with the GDPR and proposed provisions in the new Act. We want to make sure information about pupils, parents, staff and volunteers is kept secure and within the law.

What is Personal Data?

Any information that relates to a living person that identified them. This can be by name, address or phone number for example. It also relates to details about that person, which can include opinions. Some data is considered to be more sensitive, and therefore more important to protect. This is information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data, and biometric data where processed to uniquely identify a person.

Schools often collect sensitive data for DfE and LA requirements and of course pupil data may contain information about safeguarding, SEN or health needs. Information about other family members may also be on the school file.

Every school has to publish a Privacy / Fair Processing Notice on the website.

What are the key principles of the GDPR?

Lawfulness, transparency and fairness.

School must have a legitimate reason to hold the data, we explain this in the Data Privacy Notices. We often ask for consent to use data about a pupil for a particular purpose. If you wish to withdraw consent we have a form to complete to allow us to process your request. There are sometimes when you cannot withdraw consent as explained in 'Data Subjects Rights'.

Collect data for a specific purpose and use it for that purpose

Data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.

Limited collection

Data controllers should only collect the minimum amount of data needed for a particular task or reason. If there is a breach or a hack only limited information can be lost.

Accuracy

Data collected should be accurate, and steps should be taken to check and confirm accuracy. We do this when pupils join the school and check on an annual basis.

If a Data Subject feels that the information held is inaccurate, should no longer be held by the Controller or should not be held by the Controller in any event a dispute resolution process and complaint process can be accessed, using the suitable forms.

Retention

The School has a retention policy that explains how long we store records for.

Security

All forms of record that include pupil/staff identifiable information should be kept securely in locked filing cabinets, password protected electronic databases or other form of restricted access storage when not in use. This includes keeping records secure when visiting pupils in their homes. Employees are expected to take appropriate measures to ensure the security of the record at all times.

We have processes in place to keep data safe. That might be paper files, electronic records or other information. No more than one year of data is held in a secure archive room. Everything else is kept off site in a locked storage centre which is managed by the business manager.

Who is a 'data subject' ?

Someone whose details we keep on file. Some details are more sensitive than others. The GDPR sets out collection of details such as health conditions and ethnicity which are more sensitive than names and phone numbers.

Data subjects' rights

Individuals have a right:-

- to be informed
- of access to data stored about them or their children
- to rectification if there is an error on the data stored
- to erasure if there is no longer a need for school to keep the data
- to restrict processing, i.e. to limit what is done with their data
- to object to data being shared or collected

There are other rights that relate to automated decision making and data portability that are not directly relevant in schools.

Data subject's rights are also subject to child protection and safeguarding concerns, sharing information for the prevention and detection of crime. Schools also have legal and contractual obligations to share information with organisations such as the Department for Education, Social Care, the Local Authority and HMRC amongst others. In some cases these obligations override individual rights.

These Data Subject's Rights are set out in more detail in the document 'My Rights – A Guide for Data Subjects'.

Subject Access Requests

You can ask for copies of information that we hold about you or a pupil who you have parental responsibility for at school. This Subject Access Request process is set out separately. You need to fill out the form, and you may need to provide identification evidence for us to process the request.

We have to provide the information within a month, but this can be extended if, for example, the school was closed for holidays. The maximum extension is up to two months.

When we receive a request we may ask you to be more specific about the information that you require. This is to refine any queries to make sure you access what you need, rather than sometimes getting a lot of information that may not be relevant to your query.

In accordance with the Data (Use and Access) Act 2025, we are required to conduct searches that are reasonable and proportionate when responding to a SAR. If a request results in a substantial volume of data deemed to be unreasonable and disproportionate, we will notify you and offer an opportunity to refine the scope of your request. This allows you to specify the information you are seeking, enabling us to carry out a targeted search and provide the most relevant data.

In some cases we cannot share all information we hold on file if there are contractual, legal or regulatory reasons.

We cannot release information provided by a third party without their consent, or in some cases you may be better to approach them directly, e.g. school nurses who are employed by the NHS.

We will supply the information in an electronic form.

If you wish to complain about the process, please see our complaints policy (Appendix A) and later information in this GDPR policy.

Who is a 'data controller'?

Birkett House school governing body is the data controller. It has ultimate responsibility for how the school manages data. It delegates this to data processors to act on its behalf.

Who is a 'data processor'?

This is a person or organisation that uses, collects, accesses or amends the data that the controller has collected or authorised to be collected. It can be a member of staff, a third-party company, possibly a governor, a contractor or temporary employee. It can also be another organisation such as the police or the LA.

Data controllers must make sure that data processors are as careful about the data as the controller themselves. The GDPR places additional obligations on organisations to make sure that Data Controllers require contractual agreements to ensure that this is the case.

Processing data

The School must have a reason to process the data about an individual. Our privacy notices set out how we use data. The UK GDPR as amended by the Data (Use and Access) Act (DUAA) 2025 has seven conditions for lawful processing and any time we process data relating to an individual it is within one of those conditions.

If there is a data breach, we have a separate policy and procedure to follow to take immediate action to remedy the situation as quickly as possible.

The legal basis and authority for collecting and processing data in school are: -

- consent obtained from the data subject or their parent
- performance of a contract where the data subject is a party
- compliance with a legal obligation
- to protect the vital interests of the data subject or other associated person
- to carry out the processing that is in the public interest and/or official authority
- it is necessary for the legitimate interests of the data controller or third party
- in accordance with national law
- to safeguard vulnerable individuals, crime prevention, and respond to emergencies.

In addition, any special categories of personal data are processed on the grounds of:

- explicit consent from the data subject or about their child
- necessary to comply with employment rights or obligations
- protection of the vital interests of the data subject or associated person
- being necessary to comply with the legitimate activities of the school
- existing personal data that has been made public by the data subject and is no longer confidential
- bringing or defending legal claims
- safeguarding
- national laws in terms of processing genetic, biometric or health data.

Processing data is recorded within the school systems.

Data Sharing

Data sharing is done within the limits set by the GDPR. Guidance from the Department for Education, health, the police, local authorities and other specialist organisations may be used to determine whether data is shared.

The basis for sharing or not sharing data is recorded in school.

When sending sensitive information by post the following procedure should be followed:

Where the public post system is required check the name, department and address of the intended recipient. Use a robust envelope. Mark the envelope 'Private & Confidential', to be opened by addressee only'. Ensure that a return address is recorded on the outside of the envelope. If the information is considered to be highly sensitive the item should be sent by recorded delivery

Any transfers of confidential information should be secure and the method risk assessed.

Breaches & Non-Compliance

If there is noncompliance with the policy or processes, or there is a DPA breach as described within the GDPR and DPA 2018 then the guidance set out in the Breach & Non-Compliance Procedure and Process needs to be followed.

Protecting data and maintaining data subjects' rights is the purpose of this policy and associated procedures.

Consent

As a school we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required. However, in most cases data will only be processed if explicit consent has been obtained.

Consent is defined by the GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

This will be largely managed in the school.

Consent and Renewal

On the school website we have 'Privacy Notices' that explain how data is collected and used. It is important to read those notices as it explains how data is used in detail.

Obtaining clear consent and ensuring that the consent remains in place is important for school. We also want to ensure the accuracy of that information.

For Pupils and Parents/Carers

On arrival at school you will be asked to complete a form giving next of kin details, emergency contact and other essential information. We will also ask you to give consent to use the information for other in school purposes, as set out on the data collection/consent form.

We review the contact and consent form on an annual basis. It is important to inform school if details or your decision about consent changes. A form is available.

Pupil Consent Procedure

Where processing relates to a child under 13 years old, school will obtain the consent from a person who has parental responsibility for the child.

Pupil's may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent the school will consider each situation on the merits and within the principles of GDPR and also child welfare, protection and safeguarding principles.

Please complete the appropriate form.

CCTV Policy

Please also see the CCTV Policy. We use CCTV (external use only) and store images for a period of time in line with the policy. CCTV may be used for: -

- detection and prevention of crime
- to monitor entrances and exits to the building
- to assist the school in complying with legal and regulatory obligations

Data Protection Officer

We have a Data Protection Officer (DPO) whose role is to:

- inform and advise the controller or the processor and the employees who carry out processing of their obligations under the UK GDPR
- monitor compliance with the UK GDPR and DPA
- provide advice where requested about the data protection impact assessment and monitor its performance
- be the point of contact for Data Subjects if there are concerns about data protection
- cooperate with the supervisory authority and manage the breach procedure
- advise about training and CPD for the UK GDPR

Our DPO is John Walker whose contact details are below.

John Walker The Brutus Centre, Station Road, Totnes, Devon, TQ9 5RW
Email: info@phplaw.co.uk

Physical Security

As a school we are obliged to have appropriate security measures in place.

In school, every secure area has individuals who are responsible for ensuring that the space is securely maintained and controlled if unoccupied, i.e. locked. Offices and cupboards that contain personal data should be secured if the processor is not present.

Staff and Governors should ensure access to computer equipment is restricted by closing windows and doors when the appropriate room is not in use.

Equipment and paper files should not be left on view in any public setting. Computer monitors should be positioned in such a way that information stored or being processed cannot be

viewed by unauthorised persons or members of the public. As far as is practical, only authorised persons should be admitted to rooms that contain servers or provide access to data.

Lock your computer screen (Ctrl,Alt and Del) if you are leaving your desk. Mobile devices (e.g. laptops, PDA's, memory sticks, etc) must be password protected.

Any files that contain personal identifiable information should be saved onto a shared network or OneDrive and not the C: Drive.

Passwords must not be shared with other members of staff under any circumstances. Passwords must not be written down and/or left on display or be easily accessible. They should be "complex" passwords and should be changed frequently.

It is advisable to password protect any personal files in particular those that contain potentially embarrassing information about an individual or an organisation.

The Site Manager is responsible for authorising access to secure areas along with Head & Business Manager.

All Staff, contractors and third parties who have control over lockable areas must take due care to prevent data breaches.

All sites and locations need to have suitable security and review measures in place.

Secure Disposal

When disposal of items is necessary a suitable process must be used. This is to secure the data, to provide a process that does not enable data to be shared in error, by malicious or criminal intent.

These processes, when undertaken by a third party are subject to contractual conditions to ensure GDPR and DPA compliance.

Hardware is disposed / recycled by the IT department &/or reputable companies

Hard copy files are destroyed by shredding with reputable companies

Servers and Hard drives are cleansed by IT department.

Portable and removable storage are destroyed / cleaned/ recycled by IT department

Complaints & the Information Commissioner Office (ICO)

In accordance with requirements set out by DUA 2025, the school has a dedicated complaint procedure for data protection matters. The school's complaints policy is included in Appendix A.

There is a right to complain if you feel that data has been shared without consent or lawful authority.

You can complain if you have asked to us to erase, rectify, not process data and we have not agreed to your request.

We will always try to resolve issues on an informal basis, and then through our formal complaints procedure. Please complete the form, and we will contact you with more details about the

timescale and process.

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations. Email: casework@ico.org.uk Helpline: 0303 123 1113 web: www.ico.org.uk

Review

A review of the effectiveness of GDPR compliance and processes will be conducted by the Data Protection Officer every 24 months.

Appendix A

Data (Use and Access) Act 2025 - Complaint Process

Introduction

Birkett House School is committed to protecting the privacy and personal data of its students, staff, parents/carers, governors and the wider school community. This policy outlines the procedure for handling complaints related to data use and access, in accordance with the Data (Use and Access) Act (DUAA) and other relevant UK data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

The UK GDPR documents as set out on our website provide an overview of how personal data is managed across our setting/settings.

This is an appendix to the main complaint policy and reflects the requirement for standalone data use complaints to be handled using a separate procedure. Any complaint that is linked to other matters, whether raised as a formal or informal complaint are to be dealt with under the standard complaint process as outlined within the main complaint policy.

Roles and responsibilities

The Data Controller (DC) is responsible for ensuring compliance with this policy and the legal obligations imposed by the UK GDPR, Data Protection Act 2018, DUAA 2025 and other relevant legislation. The DC will delegate day-to-day management of this to the relevant staff members and the DC will expect that staff member to investigate any complaint unless there is a conflict of interest, in which case the DC will appoint a suitable person.

The headteacher and leadership team are responsible for ensuring all staff are aware of this policy and their data protection obligations.

All staff members are responsible for handling personal data in a secure and lawful manner and for co-operating fully with any investigation into a data use or access complaint.

Scope

This policy applies to all individuals who have dealings with Birkett house School and believe that their personal data has been used or accessed inappropriately, or that their rights under the DUAA and other data protection laws have been infringed.

This includes but is not limited to:

- current and former students
- parents/carers
- school staff (teaching, support, and administrative)
- governors
- volunteers
- contractors and suppliers

Principles

Fairness and transparency: All complaints will be handled in a fair, impartial, and transparent manner.

Confidentiality: Complaints and all related information will be treated with the utmost confidentiality, unless disclosure is required by law.

Timeliness: Complaints will be acknowledged and investigated in a prompt manner.

Compliance: All actions taken will comply with the DUAA, UK GDPR, DPA 2018, and other relevant legislation.

The complaint procedure

Step 1: Informal resolution

We encourage individuals to first attempt an informal resolution of their concerns. If you have a concern about data use or access, you should, in the first instance, raise it with the School Business Manager Natalie Burniston nburniston@birketthouse.leics.sch.uk

In many cases, issues can be resolved quickly and informally at this stage.

Step 2: Formal complaint submission

If the informal approach is not successful or deemed inappropriate, a formal complaint should be submitted in writing using the complaint form attached.

The complaint should be addressed to John Walker (DPO) Email: info@jawalker.co.uk

The written complaint shall include the following information:

1. your full name and contact details.
2. a clear and concise description of the complaint, including what happened, when it happened, and who was involved.
3. a description of the data involved and how you believe it was used or accessed inappropriately.
4. any relevant dates, times, or evidence.
5. details of any informal steps you have already taken to resolve the issue.
6. the desired outcome of the complaint.

Step 3: Acknowledgment and investigation

You will receive an acknowledgment of the written complaint within 5 working days of the setting receiving it.

The DC will conduct a thorough and impartial investigation into the complaint.

This may involve:

- interviewing the complainant
- interviewing relevant staff members
- reviewing school records, logs, and policies
- consulting with external legal or data protection experts if necessary

The School will aim to complete the investigation and provide a substantive response within 20 working days of the complaint's acknowledgment. If the investigation is complex and requires more time, the DC will write to the complainant to explain the reason for the delay and provide a new estimated completion date.

Response

The DC will provide a formal written response to the complainant.

This response will include:

- the findings of the investigation
- a clear and reasoned conclusion as to whether the DUAA or other data protection laws have been breached.
- details of any corrective action taken or planned to prevent a recurrence of the issue.
- the outcome of the complaint, including whether it has been upheld, partially upheld, or not upheld.
- information on the next steps available to the complainant if they remain dissatisfied.

Escalation

If the complainant is not satisfied with the school's final response, they have the right to escalate their complaint to the Information Commissioner's Office (ICO).

The ICO's contact details are as follows:

Website: <https://ico.org.uk>

Telephone: 0303 123 1113

Postal Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Policy Review

This policy will be reviewed annually by the Data Protection Officer and the school leadership team to ensure it remains relevant, effective, and compliant with all current legislation.

Date of implementation: March 2026

Review date: March 2027