



Falkner House Data Protection and Privacy Policy

Nursery - Year 6

Relevant Legislation

This policy reflects: *UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018, Privacy and Electronic Communications Regulations (PECR), Education Act 2002, Children Act 1989, Equality Act 2010, Education and Skills Act 2008, Independent School Standards Regulations 2014 (and as amended) Keeping Children Safe in Education (current edition)*

Relevant Legislation	1
Policy Statement	2
Scope	2
Data Protection Principles	3
Responsibility for Data Protection	3
Categories of Personal Data	3
Pupils	3
Parents	3
Staff and Volunteers	4
Lawful Bases for Processing	4
Why The School Needs to Process Personal Data	4
How The School Collects Data	6
Who Has Access to Personal Data and Who The School Shares it With	6
International Data Transfers	7
The National Pupil Database (Npd)	7
Data Retention	7
Data Security	8
Personal Data Breaches	8
Keeping In Touch	8
Your Rights	9
Whose Rights	10
Data Accuracy	10
Queries And Complaints	11



Policy Statement

Falkner House LLP (“the School”) is committed to protecting the privacy, confidentiality and security of personal data. The School processes personal information in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and all other applicable data protection legislation.

The School recognises the importance of maintaining trust and confidence with pupils, parents, staff, governors, volunteers, contractors and visitors and is committed to processing personal data fairly, lawfully, transparently and securely.

Falkner House LLP is registered in England and Wales under company number OC370021 and acts as the Data Controller for the personal data it processes.

Falkner House operates on two sites:

19 Brechin Place – for girls aged 4 – 11 and a nursery School for boys and girls aged 3 – 4.

20 Penywern Road - for boys aged 4 – 11.

Scope

This policy applies to:

- Current, former and prospective pupils
- Parents, guardians and carers
- Employees
- Volunteers
- Contractors and consultants
- Visitors
- Alumni

This policy should be read alongside:

- Child Protection and Safeguarding Policy
- Staff Code of Conduct
- Online Safety Policy
- Internet Policy
- Records Retention Schedule
- Recruitment and Safer Recruitment Procedures
- Complaints Policy and Procedure

Data Protection Principles

The School will ensure personal data is:

- Processed only where there is a lawful basis.
- Used only for legitimate educational, employment, safeguarding or operational purposes.



- Only information necessary for the purpose will be collected.
- Reasonable steps will be taken to keep information accurate and up to date.
- Information will be retained according to the School's Records Retention Schedule.
- Appropriate technical and organisational measures will protect personal data.
- The School will demonstrate compliance with data protection legislation.

Responsibility for Data Protection

The School has appointed the Bursar as its Data Protection Lead (DPL).

The DPL is responsible for:

- Monitoring compliance
- Managing subject access requests
- Coordinating responses to data breaches
- Maintaining data protection procedures
- Advising staff on data protection matters
- Liaising with the Information Commissioner's Office (ICO)

All staff are responsible for protecting personal data and complying with this policy.

Categories of Personal Data

The School may process:

Pupils

- Names and contact details
- Date of birth
- Admission records
- Attendance records
- Assessment and examination results
- Behaviour records
- SEND information
- Safeguarding records
- Medical information
- Photographs and videos

Parents

- Contact details
- Relationship to child
- Financial information
- Emergency contact information
- Correspondence with the School

Staff and Volunteers

- Employment records
- Payroll information
- Pension information



- Recruitment documentation
- Qualifications
- References
- DBS information
- Performance management records
- Occupational health information

Lawful Bases for Processing

The School processes personal data under one or more of the following lawful bases:

- To fulfil obligations under parent contracts and employment contracts.
- To comply with education, safeguarding, employment and taxation legislation.
- To operate and manage the School effectively.
- To protect health, safety and welfare.
- Where required by law, such as certain uses of photographs or marketing communications.

Special category data is processed in accordance with Article 9 UK GDPR and relevant safeguarding, employment and education legislation.

Why The School Needs to Process Personal Data

In order to carry out its ordinary duties to staff, pupils and parents, the School may process a wide range of personal data about individuals (including current, past and prospective staff, pupils or parents) as part of its daily operation.

Some of this activity the School will need to carry out in order to fulfil its legal rights, duties or obligations – including those under a contract with its staff, or parents of its pupils.

Other uses of personal data will be made in accordance with the School's legitimate interests, or the legitimate interests of another, provided that these are not outweighed by the impact on individuals, and provided it does not involve special or sensitive types of data.

The School expects that the following uses may fall within that category of its (or its community's) "legitimate interests":

- for the purposes of pupil selection (and to confirm the identity of prospective pupils and their parents);
- to provide education services, including musical education, physical training or spiritual development, and extra-curricular activities to pupils, and monitoring pupils' progress and educational needs;
- to assess the quality of service;
- maintaining relationships with alumni and the School community;
- for the purposes of management planning and forecasting, research and statistical analysis, including that imposed or provided for by law (such as diversity or gender pay gap analysis and taxation records);
- to enable relevant authorities to monitor the School's performance and to intervene or assist with incidents as appropriate;



- to give and receive information and references about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational institution that the pupil attended or where it is proposed they attend; and to provide references to potential employers of past pupils;
- to enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the School;
- to safeguard pupils' welfare and provide appropriate pastoral care;
- to monitor (as appropriate) use of the School's IT and communications systems in accordance with the School's IT's policy;
- to make use of photographic images of pupils in School publications, on the School website in accordance with the School's policy on taking, storing and using images of children;
- where necessary for the School's purposes, including to obtain appropriate professional advice and insurance for the School.

In addition, the School may need to process special category personal data (e.g health, ethnicity, religion or criminal records information (e.g. when carrying out DBS checks) in accordance with rights or duties imposed on it by law, including as regards safeguarding and employment, or from time to time by explicit consent where required.

These reasons may include:

- to safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency, incident or accident, including by disclosing details of an individual's medical condition where it is in the individual's interests to do so: e.g. for medical advice, social services, insurance purposes or to organisers of School trips;
- to provide educational services in the context of any special educational needs of a pupil;
- in connection with employment of its staff, for example DBS checks, welfare or pension plans; or
- for legal and regulatory purposes (e.g .child protection, diversity monitoring and health and safety) and to comply with its legal obligations and duties of care.

How The School Collects Data

Generally, the School receives personal data from the individual directly (including, in the case of pupils, from their parents). This may be via a form, or simply in the ordinary course of interaction or communication (such as email or written assessments).

In some cases, personal data may be supplied by third parties (for example another School, or other professionals or authorities working with that individual); or collected from publicly available resources.



Who Has Access to Personal Data and Who The School Shares it With

Occasionally, the School will need to share personal information relating to its community with third parties, such as professional advisers (lawyers and accountants), schools that pupil's attend after leaving, Department for Education (DfE) or relevant authorities (HMRC, police or the local authority).

For the most part, personal data collected by the School will remain within the School, and will be processed by appropriate individuals only in accordance with access protocols (i.e. on a 'need to know' basis).

Particularly strict rules of access apply in the context of:

- medical records; and
- pastoral or safeguarding files.

However, some of a pupil's relevant information will need to be provided to staff more widely in the context of providing the necessary care and education that the pupil requires.

Staff, pupils and parents are reminded that the School is under duties imposed by law and statutory guidance (including Keeping Children Safe in Education (current edition) to record or report incidents and concerns that arise or are reported to it, in some cases regardless of whether they are proven, if they meet a certain threshold of seriousness in their nature or regularity. This may include file notes on personnel or safeguarding files, and in some cases referrals to relevant authorities such as the LADO or police. For further information about this, please view the Falkner House Child Protection Safeguarding Policy.

Information will only be shared where there is a lawful basis to do so.

International Data Transfers

Where personal data is transferred outside the United Kingdom, the School will ensure that appropriate safeguards are in place including:

- UK adequacy regulations
- International Data Transfer Agreements (IDTAs)
- Standard contractual clauses
- Other lawful transfer mechanisms approved under UK GDPR

The National Pupil Database (Npd)

The NPD is owned and managed by the Department for Education (DfE) and contains information about pupils in schools in England. It is held in electronic format for statistical purposes and is securely collected from a range of sources including schools, local authorities and awarding bodies. The School is required by law, Education (Information About Individual Pupils) (England) Regulations 2013) to provide information about



our pupils to the DfE as part of statutory data collections such as the School census and early years' census. <https://www.gov.uk/education/data-collection-and-censuses-for-Schools>.

<https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>.

The DfE <https://www.gov.uk/contact-dfe> may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England. The DfE has robust processes in place to ensure the confidentiality of data is maintained and there are stringent controls in place regarding access and the use of the data. <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>. For information about which organisations the department has provided pupil information, (and for which project), please visit the following website;

<https://www.gov.uk/government/publications/national-pupil-database-requests-received>.

Data Retention

The School will retain personal data securely and only in line with how long it is necessary to keep for a legitimate and lawful reason. Typically, the legal recommendation for how long to keep ordinary staff and pupil personnel files is up to 7 years following departure from the School. However, retention periods may vary according to safeguarding obligations, educational requirements, employment legislation and limitation periods. Records will be securely destroyed when no longer required.

Data Security

The School will take appropriate technical and organisational steps to ensure the security of personal data about individuals, including policies around use of technology and devices, and access to School systems. All staff and governors will be made aware of this policy and their duties under Data Protection Law and receive relevant training. Access to personal data is restricted on a need-to-know basis.

The School implements appropriate technical and organisational measures including:

- Secure IT systems
- Access controls and Password protection
- Encryption where appropriate
- Secure disposal arrangements
- Staff training
- Confidentiality requirements

Personal Data Breaches

Staff must report any actual or suspected data breach immediately to the Data Protection Lead. The school will investigate all breaches and will, if any breaches are found, submit reports to the Information Commissioners Office (ICO) within 72 hours. All breaches will be recorded in a Data Breach Register.



Keeping In Touch

The School will use the contact details of parents, alumni and other members of the School community to keep them updated about the activities of the School, or alumni and parent events of interest, including by sending updates and newsletters, by email and by post. Should you wish to limit or object to any such use, or would like further information about them, please contact the DPL in writing. However, the School may nonetheless need to retain some of your details (not least to ensure that no more communications are sent to that particular address, email or telephone number).

Your Rights

Individuals have various rights under Data Protection Law to access and understand personal data about them held by the School, and in some cases ask for it to be erased or amended or for the School to stop processing it, but subject to certain exemptions and limitations. Any individual wishing to access or amend their personal data, or wishing it to be transferred to another person or organisation, should put their request in writing to the DPL.

The School will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event within statutory time-limits, which is one month in the case of requests for access to information. The School will be better able to respond quickly to smaller, targeted requests for information. If the request is manifestly excessive or similar to previous requests, the School may ask you to reconsider or charge a proportionate fee, but only where Data Protection Law allows it.

You should be aware that certain data is exempt from the right of access. This may include information which identifies other individuals, or information which is subject to legal professional privilege. The School is also not required to disclose any pupil examination scripts (though examiners' comments may fall to be disclosed), nor any confidential reference given by the School for the purposes of the education, training or employment of any individual.

Pupils can make subject access requests for their own personal data, provided that, in the reasonable opinion of the School, they have sufficient maturity to understand the request they are making (see section Whose Rights below). Indeed, while a person with parental responsibility will generally be expected to make a subject access request on behalf of younger pupils, the information in question is always considered to be the child's at law. A pupil of any age may ask a parent or other representative to make a subject access request on his/her behalf, and moreover (if of sufficient age) their consent or authority may need to be sought by the parent. Pupils aged 13 are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested, including any relevant circumstances at home. Children younger than 13 may be sufficiently mature to have a say in this decision. All subject access requests from pupils will therefore be considered on a case by case basis.



Where the School is relying on consent as a means to process personal data, any person may withdraw this consent at any time (subject to similar age considerations as above). Please be aware however that the School may have another lawful reason to process the personal data in question even without your consent.

That reason will usually have been asserted under this DPPP or may otherwise exist under some form of contract or agreement with the individual (e.g. an employment or parent contract, or because a purchase of goods, services or membership of an organisation has been requested).

Whose Rights

The rights under Data Protection Law belong to the individual to whom the data relates. However, the School will often rely on parental consent to process personal data relating to pupils (if consent is required) unless, given the nature of the processing in question, and the pupil's age and understanding, it is more appropriate to rely on the pupil's consent.

Parents should be aware that in such situations they may not be consulted, depending on the interests of the child, the parents' rights at law or under their contract, and all the circumstances. In general, the School will assume that pupils' consent is not required for ordinary disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the pupil's activities, progress and behaviour, and in the interests of the pupil's welfare, unless, in the School's opinion, there is a good reason to do otherwise.

However, where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, the School may be under an obligation to maintain confidentiality unless, in the School's opinion, there is a good reason to do otherwise; for example where the School believes disclosure will be in the best interests of the pupil or other pupils, or if required by law.

Pupils are required to respect the personal data and privacy of others, to comply with the School's Internet Security and Code of Conduct Policy and School rules.

Data Accuracy

The School will endeavour to ensure that all personal data held in relation to an individual is as up to date and accurate as possible. Individuals must please notify the appropriate Bursar of any changes to information held about them.

An individual has the right to request that any inaccurate or out-of-date information about them is erased or corrected (subject to certain exemptions and limitations under Act): please see above.



Queries And Complaints

Please see also the Falkner House Complaints Policy

Any comments or queries on this policy should be directed to the Bursar who is the DPL using the contact details office@falknerhouse.co.uk (Brechin Place) or office20pr@falknerhouse.co.uk (Penywern Road)

If an individual believes that the School has not complied with this policy or acted otherwise than in accordance with Data Protection Law, they should utilise the School complaints / grievance procedure and should also notify the DPL. The School can also make a referral to or lodge a complaint with the Information Commissioner's Office (ICO), although the ICO recommends that steps are taken to resolve the matter with the School before involving the regulator. <https://ico.org.uk/concerns/>