Data Protection Policy

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

1. Aims

The Friary School aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation & Guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

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 (Student Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, individual. This may include the individual's: (i) Name (including initials); (ii) Identification number; (iii) Location data; (iv) Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special Categories of Personal Data	Personal data which is more sensitive and so needs more protection, including information about an individual's: (i) Racial or ethnic origin; (ii) Political opinions; (iii) Religious or philosophical beliefs; (iv) Trade union membership; (v) Genetics; (vi) Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes; (vii) Health - physical and / or mental; (viii) Sex life or sexual orientation.
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data Subject	The identified or identifiable individual whose personal data is held or processed.
Data Controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data Processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

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

4. The Data Controller

Our school processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles & Responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing Body

The Governing Body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Pat Hunt and is contactable via Lisa Pratt, Clerk to Governors on office@friaryschool.com.

5.3 Headteacher

The Headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy.
- Informing the school of any changes to their personal data, such as a change of address.

Contacting the DPO in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
- If they have any concerns that this policy is not being followed.
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area.
- If there has been a data breach.
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
- If they need help with any contracts or sharing personal data with third parties.

6. Data Protection Principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.

This policy sets out how the school aims to comply with these principles.

7. Collecting Personal Data

7.1 Lawfulness, Fairness & Transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract.
- The data needs to be processed so that the school can **comply with a legal obligation**.
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life.
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions.
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden).
- The individual (or their parent / carer when appropriate in the case of a student) has freely given clear **consent**.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the student is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, Minimisation & Accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's Record Retention Schedule.

8. Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a student or parent / carer that puts the safety of our staff at risk.
- We need to liaise with other agencies - we will seek consent as necessary before doing this.

Our suppliers or contractors need data to enable us to provide services to our staff and students - for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and / or fraud.
- The apprehension or prosecution of offenders.
- The assessment or collection of tax owed to HMRC.
- In connection with legal proceedings.
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject Access Requests & Other Rights of Individuals

9.1 Subject Access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data concerned.
- Who the data has been, or will be, shared with.
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period.
- The source of the data, if not the individual.
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- Name of individual.
- Correspondence address.
- Contact number and email address.

- Details of the information requested.

If staff receive a subject access request they must immediately forward it to the DPO.

9.2 Children & Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our school may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification.
- May contact the individual via phone to confirm the request was made.
- Will respond without delay and within 1 month of receipt of the request.
- Will provide the information free of charge.
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the student or another individual.
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Is contained in adoption or parental order records.
- Is given to a court in proceedings concerning the child.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other Data Protection Rights of the Individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see Section 7), individuals also have the right to:

- Withdraw their consent to processing at any time.
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances).
- Prevent use of their personal data for direct marketing.
- Challenge processing which has been justified on the basis of public interest.
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area.

- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them).
- Prevent processing that is likely to cause damage or distress.
- Be notified of a data breach in certain circumstances.
- Make a complaint to the ICO.
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO via Lisa Pratt, Clerk to the Governors.

10. Parental Requests to See the Educational Record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a student) within 15 school days of receipt of a written request.

11. Biometric Recognition Systems

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use finger prints to receive school dinners instead of paying with cash we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents / carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents / carers and students have the right to choose not to use the school's biometric system. We will provide alternative means of accessing the relevant services for those students. For example, students can pay for school dinners by alternative means if they wish.

Parents / carers and students can object to participation in the school's biometric recognition system, or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s) / carer(s).

Where staff members or other adults use the school's biometric system, we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object.

Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded.

Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Ian Rose, Deputy Headteacher.

13. Photographs & Videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents / carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and / or video will be used to both the parent / carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and / or video will be used.

All schools add and adapt to reflect your school's uses of photographs and videos for communication, marketing and promotional materials.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns.
- Online on our school website or social media pages.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our Safeguarding Policy for more information on our use of photographs and videos.

14. Data Protection by Design & Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see Section 6).
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.

In addition, we will maintain records of processing activities including:

- For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices).
- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

15. Data Security & Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

This includes:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use or are password protected.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice / display boards, or left anywhere else where there is general access.
- Where personal information needs to be taken off site, staff must sign it in and out from the school office.
- Passwords that are robust are used to access school computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Staff Code of Conduct).
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see Section 8).

16. Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

Our Record Retention Schedule is based on the Information & Records Management Society's Toolkit for Schools (Version 5 - Feb 2016) and sets out how long we keep information about students.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal Data Breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of students eligible for the student premium.
- Safeguarding information being made available to an unauthorised person.
- The theft of a school laptop containing non-encrypted personal data about students.

18. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

19. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy - in liaison with the Headteacher and the Governing Body.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) - if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full Governing Body.

Note: the 2-year review frequency here reflects the information in the Department for Education's advice on statutory policies. While the GDPR and Data Protection Act 2018 (when in place) are still new and schools are working out how best to implement them, you may wish to review your data protection policy annually, and then extend this to every 2 years once you are confident with your arrangements.

20. Links with Other Policies

This data protection policy is linked to our:

- Freedom of Information Publication Scheme
- Safeguarding Policy
- SEND Policy
- Pupil Premium Policy
- Appraisal Policy
- Behaviour Policy
- Complaints Policy
- Acceptable Use of ICT Policy
- Supporting Students with Medical Conditions Policy

Reviewed By	Full Governing Body	**Implementation Date**	June 2018	**Review Date**	June 2020

Appendix 1: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.

The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

The DPO will alert the Headteacher and the Chair of Governors.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure).

The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.

The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (eg - emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system in the remit of Lisa Pratt, Clerk to Governors.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will notify any relevant third parties who can help mitigate the loss to individuals - for example, the police, insurers, banks or credit card companies

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the school's computer system in the remit of Lisa Pratt, Clerk to Governors.

The DPO and the Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Examples of School Responses to Data Breaches

Eg - Actions to Minimise the Impact of Data Breaches:

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Eg - Sensitive Information Being Disclosed via Email (including safeguarding records):

If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error

If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it.

In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.

The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher / website owner or administrator to request that the information is removed from their website and deleted.

Eg - A School Laptop or USB Containing Non-Encrypted Sensitive Personal Data Being Stolen or Hacked:

We will seek to identify the precise content of the data breach and make all formal notifications; such as to the DPO, the IOC, the local police and any named individuals known to be affected by the data breach.

The DPO will pursue all steps to relocate / return the item so that the personal data comes back under the school remit.

Members of staff responsible for the data breach will meet with the Headteacher and the incident will be reviewed as part of the Staff Disciplinary Policy.

Privacy Notice for Parents / Carers

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about students.

We, (The Friary School, Eastern Avenue, Lichfield, Staffordshire, WS13 7EW), are the 'data controller' for the purposes of data protection law.

Our Data Protection Officer is Pat Hunt (see 'Contact Us' below).

What Personal Data Do We Hold ?

Personal data that we may collect, use, store and share (when appropriate) about students includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Results of internal assessments and externally set tests
- Student and curricular records
- Characteristics, such as eligibility for free school meals, or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in school
- Biometric data for school canteen

We may also hold data about students that we have received from other organisations, including other schools, local authorities and the Department for Education.

Why Do We Use This Data ?

We use this data to:

- Support student learning
- Monitor and report on student progress
- Provide appropriate pastoral care
- Protect student welfare
- Assess the quality of our services
- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing

What Is Our Legal Basis For Using this Data ?

We only collect and use students' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process students' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)
- Where we have obtained consent to use students' personal data, this consent can be withdrawn at any time
- We will make this clear when we ask for consent, and explain how consent can be withdrawn

Some of the reasons listed above for collecting and using students' personal data overlap, and there may be several grounds which justify our use of this data.

How Do We Collect Information ?

While the majority of information we collect about students is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How Do We Store This Data ?

We keep personal information about students while they are attending our school.

We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations.

Our Record Retention Schedule is based on the Information & Records Management Society's Toolkit for Schools (Version 5 - Feb 2016) and sets out how long we keep information about students.

A copy of our Record Retention Schedule is available from Lisa Pratt, Clerk to Governors, via office@friaryschool.com.

Who Do We Share Data With ?

We do not share information about students with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about students with:

Staffordshire County Council	To meet our legal obligations to share certain information with it; such as safeguarding concerns, exclusions and attendance.
Department for Education	To meet our legal obligations to share certain information with it; such as census records.
Educating Bodies	To provide information to support student learning; such as online learning packages and intervention analysis and support.
Examining Bodies	To provide information to support entry and support in taking formal exams.
OFSTED	To provide information to our regulator to support their evaluative work of our provision; such as student outcomes.
Suppliers & Service Providers	To enable them to provide the service we have contracted them for; such as biometric data for canteen payments.
Financial Organisations	To enable them to provide the financial support that assists the school in securing best possible funding and provision.

Auditors	To provide information to support the analysis and evaluation that assists the school in securing best possible spending and provision.
Survey & Research Organisations	To provide information to support school self-evaluation and to inform teaching and learning approaches.
Health Authorities & Bodies	To enable health authorities to effectively deliver key health provision to students; such as vaccinations and referrals.
Security Organisations	To enable providers to maintain security and safety for all students; such as biometric data for canteen payments.
Social Welfare Organisations	To enable social welfare providers to effectively deliver key provision to students; such as mentoring and referrals.
Professional Consultants	To provide information to support student learning; such as cohort specific data and intervention analysis and support.
Charity / Voluntary Organisations	To provide information to support student learning and engagement; such as press releases and support packages.
Judiciary & Policing Bodies	To meet our legal obligations to share certain information with it; such as criminal concerns or legislative matters.
Professional Bodies	To provide information to support school self-evaluation and to inform teaching, learning and pastoral approaches.

What Is The National Student Database ?

We are required to provide information about students to the Department for Education as part of statutory data collections such as the school census.

Some of this information is then stored in the National Student Database (NPD), which is owned and managed by the Department of Education and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use the data.

For more information, see the Department's webpage on how it collects and shares research data.

You can also contact the Department for Education with any further questions about the NPD.

How Do We Meet Legal Requirements Relating to Education & Training for 13+ Students ?

Once our students reach the age of 13, we are legally required to pass on certain information about them to Staffordshire County Council, as it has legal responsibilities regarding the education or training of 13-19 year-olds.

This information enables it to provide youth support services, Post-16 education and training services, and careers advisers.

Parents / carers, or students once aged 16 or over, can contact our Data Protection Officer to request that we only pass the individual's name, address and date of birth to Staffordshire County Council.

How Do We Transfer Data Internationally ?

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

What Are Parents & Students Rights Regarding Personal Data ?

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them.

Parents / carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

- If you make a subject access request, and if we do hold information about you or your child, we will:
- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request please contact our Data Protection Officer by directing your query to Lisa Pratt, Clerk to Governors, via office@friaryschool.com.

Parents / carers also have a legal right to access to their child's **educational record**. To request access, please contact Lisa Pratt, Clerk to Governors, via office@friaryschool.com.

What Other Rights Are Important ?

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our Data Protection Officer by directing your query to Lisa Pratt, Clerk to Governors, via office@friaryschool.com.

How Can You Make A Complaint ?

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our Data Protection Officer by directing your query to Lisa Pratt, Clerk to Governors, via office@friaryschool.com.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

How Can You Contact Us ?

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection Officer:

- Mrs Pat Hunt, C/O Lisa Pratt (Clerk to Governors), The Friary School, Eastern Avenue, Lichfield, Staffordshire, WS13 7EW.

Contact can be made in writing either via this postal address or by emailing office@friaryschool.com.

References:

This notice is based on the Department for Educations model privacy notice, amended for parents and to reflect the way we use data in this school.

Additionally, the following documents have been consulted in writing this Privacy Notice:

- The Information Commissioner Office's Check-List

  https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

- The Information Commissioner Office's Definitions of 'Personal Data' and 'Special Categories of Personal Data'

  https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/

- The Information Commissioner Office's Guidance on the Lawful Basis for Processing

  https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing

- The Information & Records Management Society's Toolkit for Schools

  https://irms.org.uk/page/schoolstoolkit?&terms=%22toolkit+and+schools%22

- The National Pupil Database: User Guide & Supporting Information

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

- DfE Guidance - Data Protection: How We Share Pupil & Workforce Data

  https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data

- DfE Model Privacy Notices

  https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

Privacy Notice for Students

You have a legal right to be informed about how our school uses any personal information that we hold about you.

To comply with this, we provide a 'privacy notice' to you where we are processing your personal data.

This privacy notice explains how we collect, store and use personal data about you.

We, (The Friary School, Eastern Avenue, Lichfield, Staffordshire, WS13 7EW), are the 'data controller' for the purposes of data protection law.

Our Data Protection Officer is Pat Hunt (see 'Contact Us' below).

What Personal Data Do We Hold ?

We hold some personal information about you to make sure we can help you learn and to look after you at school.

For the same reasons, we get information about you from some other places too - like other schools, the local council and the government.

This information includes:

- Your contact details
- Your test and exam results
- Your attendance records
- You characteristics, like you ethnic background or any special educational needs or disabilities
- Any medical conditions you have
- Details of any behaviour issues or exclusions
- Photographs
- CCTV images
- Biometric data (for school canteen)

Why Do We Use This Data ?

We use this data to help run the school, including to:

- Get in touch with you and your parents when we need to
- Check how you're doing in exams an work out whether you or your teachers need any extra help
- Track how well the school as a whole is performing
- Look after your well-being

What Is Our Legal Basis For Using this Data ?

We only collect and use your information when the law allows us to. Most often, we will use your information where:

- We need to comply with the law
- We need to use it to carry out a task in the public interest (in order to provide you with an education)

Sometimes, we may also use your personal information where:

- You, or your parents / carers, have given us permission to use it in a certain way
- We need to protect your interests (or someone else's interests)

Where we have got permission to use your data, you or your parents / carers may withdraw this at any time. We will make this clear when we ask for permission, and explain how to go about withdrawing consent.

Some of the reasons listed above for collecting and using your information overlap, and there may be several grounds which mean we can use your data.

How Do We Collect Information ?

While in most cases you, or your parents / carers, must provide the personal information we need to collect, there are some occasions when you can choose whether or not to provide the data.

We will always tell you if it's optional. If you must provide the data, we will explain what might happen if you don't.

How Do We Store This Data ?

We keep personal information about you while you are a student at our school.

We may also keep it after you have left the school, where we are required by law.

We have a Record Retention Schedule which sets out how long we must keep information about you

A copy of our Record Retention Schedule - based on the Information & Records Management Society's Toolkit for Schools (Version 5 - Feb 2016) - is available from Lisa Pratt, Clerk to Governors, via office@friaryschool.com.

Who Do We Share Data With ?

We do not share personal information about you with anyone outside the school without permission from you or your parents / carers, unless the law and our policies allow us to do so.

Where it is legally required, or necessary for another reason allowed under data protection law, we may share personal information about you with:

Staffordshire County Council	To meet our legal obligations to share certain information with it; such as safeguarding concerns, exclusions and attendance.
Department for Education	To meet our legal obligations to share certain information with it; such as census records.
Educating Bodies	To provide information to support student learning; such as online learning packages and intervention analysis and support.
Examining Bodies	To provide information to support entry and support in taking formal exams.
OFSTED	To provide information to our regulator to support their evaluative work of our provision; such as student outcomes.
Suppliers & Service Providers	To enable them to provide the service we have contracted them for; such as biometric data for canteen payments.
Financial Organisations	To enable them to provide the financial support that assists the school in securing best possible funding and provision.
Auditors	To provide information to support the analysis and evaluation that assists the school in securing best possible spending and provision.
Survey & Research Organisations	To provide information to support school self-evaluation and to inform teaching and learning approaches.

Health Authorities & Bodies	To enable health authorities to effectively deliver key health provision to students; such as vaccinations and referrals.
Security Organisations	To enable providers to maintain security and safety for all students; such as biometric data for canteen payments.
Social Welfare Organisations	To enable social welfare providers to effectively deliver key provision to students; such as mentoring and referrals.
Professional Consultants	To provide information to support student learning; such as cohort specific data and intervention analysis and support.
Charity / Voluntary Organisations	To provide information to support student learning and engagement; such as press releases and support packages.
Judiciary & Policing Bodies	To meet our legal obligations to share certain information with it; such as criminal concerns or legislative matters.
Professional Bodies	To provide information to support school self-evaluation and to inform teaching, learning and pastoral approaches.

What Is The National Student Database ?

We are required to provide information about you to the Department for Education (a government department) as part of data collections such as the school census.

Some of this information is then stored in the National Student Database which is managed by the Department of Education and provides evidence on how schools are performing. This, in turn, supports research.

The database is held electronically so it can easily be turned into statistics. The information it holds is collected securely from schools, local authorities, exam boards and others.

The Department for Education may share information from the database with other organisations which promote children's education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use your data.

You can find out more information about this on the Department for Education's webpage on how it collects and shares research data.

You can also contact the Department for Education if you have any questions about the database.

How Do We Meet Legal Requirements Relating to Education & Training for 13+ Students ?

Once you reach the age of 13, we are legally required to pass on certain information about you to Staffordshire County Council, as it has legal responsibilities regarding the education or training of 13-19 year-olds.

This information enables it to provide youth support services, Post-16 education and training services, and careers advisers.

Your parents / carers, or you once you're 16, can contact our Data Protection Officer to ask us to only pass your name, address and date of birth to Staffordshire County Council.

How Do We Transfer Data Internationally ?

Where we share data with an organisation outside the European Economic Area, we will protect your data by following data protection law.

What Are Parents & Students Rights Regarding Personal Data ?

You can find out if we hold any personal information about you, and how we use it, by making a 'subject access request', as long as we judge that you can properly understand your rights and what they mean.

If we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and using it, and how long we will keep it for
- Explain where we got it from, if not from you or your parents
- Tell you who it has been, or will be, shared with
- Let you know if we are using your data to make any automated decisions (decisions being taken by a computer or machine, rather than by a person)
- Give you a copy of the information

You may also ask us to send your personal information to another organisation electronically in certain circumstances.

If you want to make a request please contact our Data Protection Officer by directing your query to Lisa Pratt, Clerk to Governors, via office@friaryschool.com.

What Other Rights Are Important ?

You have other rights over how your personal data is used and kept safe, including the right to:

- Say that you don't want it to be used if this would cause, or is causing, harm or distress
- Stop it being used to send you marketing materials
- Say that you don't want it used to make automated decisions (decisions made by a computer or machine, rather than by a person)
- Have it corrected, deleted or destroyed if it is wrong, or restrict our use of it
- Claim compensation if the data protection rules are broken and this harms you in some way

To exercise any of these rights, please contact our Data Protection Officer by directing your query to Lisa Pratt, Clerk to Governors, via office@friaryschool.com.

How Can You Make A Complaint ?

We take any complaints about how we collect and use your personal data very seriously, so please let us know if you think we've done something wrong.

You can make a complaint at any time by contacting our Data Protection Officer by directing your query to Lisa Pratt, Clerk to Governors, via office@friaryschool.com.

You can also complain to the Information Commissioner's Office in one of the following ways:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

How Can You Contact Us ?

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection Officer:

- Mrs Pat Hunt, C/O Lisa Pratt (Clerk to Governors), The Friary School, Eastern Avenue, Lichfield, Staffordshire, WS13 7EW.

Contact can be made in writing either via this postal address or by emailing office@friaryschool.com.

References:

This notice is based on the Department for Educations model privacy notice, amended for students and to reflect the way we use data in this school.

Additionally, the following documents have been consulted in writing this Privacy Notice:

- The Information Commissioner Office's Check-List

  https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

- The Information Commissioner Office's Definitions of 'Personal Data' and 'Special Categories of Personal Data'

  https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/

- The Information Commissioner Office's Guidance on the Lawful Basis for Processing

  https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing

- The Information & Records Management Society's Toolkit for Schools

  https://irms.org.uk/page/schoolstoolkit?&terms=%22toolkit+and+schools%22

- The National Pupil Database: User Guide & Supporting Information

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

- DfE Guidance - Data Protection: How We Share Pupil & Workforce Data

  https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data

- DfE Model Privacy Notices

  https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

Privacy Notice for Staff

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our school.

We, (The Friary School, Eastern Avenue, Lichfield, Staffordshire, WS13 7EW), are the 'data controller' for the purposes of data protection law.

Our Data Protection Officer is Pat Hunt (see 'Contact Us' below).

What Personal Data Do We Hold ?

We process data relating to those we employ, or otherwise engage, to work at our school.

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Copy of driving licence
- Photographs
- CCTV footage
- Biometric data for school canteen
- Data about your use of the school's information and communications system

We process data relating to those we employ, or otherwise engage, to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

Why Do We Use This Data ?

The purpose of processing this data is to help us run the school, including to:

- Enable you to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils

- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body

What Is Our Legal Basis For Using this Data ?

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)

Where you have provided us with consent to use your data, you may withdraw this consent at any time.

We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the school's use of your data.

How Do We Collect Information ?

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How Do We Store This Data ?

We create and maintain an employment file for each staff member.

The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.

Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our Record Retention Schedule - based on the Information & Records Management Society's Toolkit for Schools - which sets out how long we keep information about students.

A copy of our Record Retention Schedule is available from Lisa Pratt, Clerk to Governors, via office@friaryschool.com.

Who Do We Share Data With ?

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.
Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

Your Family or Representatives	To provide information relating to your / your family's welfare; such as during illness.
Staffordshire County Council	To meet our legal obligations to share certain information with it; such as safeguarding concerns.
Department for Education	To meet our legal obligations to share certain information with it; such as employment records.
Educating Bodies	To provide information to support student learning; such as online learning packages and intervention analysis and support.
Examining Bodies	To provide information to support students entry and support in taking formal exams / completing coursework.
OFSTED	To provide information to our regulator to support their evaluative work of our provision; such as staffing levels.
Suppliers & Service Providers	To enable them to provide the service we have contracted them for; such as for payroll and pensions.
Financial Organisations	To enable them to provide the financial support that assists the school in securing best possible provision.
Auditors	To provide information to support the analysis and evaluation that assists the school in securing best possible provision.
Trade Unions & Associations	To provide information to support trade union support; such as disciplinary matters.
Survey & Research Organisations	To provide information to support school self-evaluation and to inform teaching and learning approaches.
Security Organisations	To enable providers to maintain security and safety for all staff; such as biometric data for canteen payments.
Social Welfare Organisations	To enable social welfare providers to effectively deliver key provision to staff; such as counselling referrals.
Professional Consultants	To provide information to support staff welfare and delivery; such as Occupational Health professionals or teaching training bodies.
Charity / Voluntary Organisations	To provide information to support staff engagement; such as press releases and support packages.
Judiciary & Policing Bodies	To meet our legal obligations to share certain information with it; such as criminal concerns or legislative matters.
Professional Bodies	To provide information to support school self-evaluation and to inform teaching, learning and pastoral approaches.
Employment & Recruitment Agencies	To provide information relating to length of services and professional conduct; such as for references.

How Do We Transfer Data Internationally ?

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

What Are Staff Rights Regarding Personal Data ?

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them.

- If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request please contact our Data Protection Officer by directing your query to Lisa Pratt, Clerk to Governors, via office@friaryschool.com.

What Other Rights Are Important ?

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe.

You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our Data Protection Officer by directing your query to Lisa Pratt, Clerk to Governors, via office@friaryschool.com.

How Can You Make A Complaint ?

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our Data Protection Officer by directing your query to Lisa Pratt, Clerk to Governors, via office@friaryschool.com.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

How Can You Contact Us ?

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection Officer:

- Mrs Pat Hunt, C/O Lisa Pratt (Clerk to Governors), The Friary School, Eastern Avenue, Lichfield, Staffordshire, WS13 7EW.

Contact can be made in writing either via this postal address or by emailing office@friaryschool.com.

References:

This notice is based on the Department for Educations model privacy notice, amended for staff and to reflect the way we use data in this school.

Additionally, the following documents have been consulted in writing this Privacy Notice:

- The Information Commissioner Office's Check-List

  https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

- The Information Commissioner Office's Definitions of 'Personal Data' and 'Special Categories of Personal Data'

  https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/

- The Information Commissioner Office's Guidance on the Lawful Basis for Processing

  https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing

- The Information & Records Management Society's Toolkit for Schools

  https://irms.org.uk/page/schoolstoolkit?&terms=%22toolkit+and+schools%22

- DfE Guidance - Data Protection: How We Share Pupil & Workforce Data

  https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data

- DfE Model Privacy Notices

  https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices