Privacy Notice – Staff

Franklin College Trust is committed to protecting and respecting the privacy of all our staff's personal data whilst at the Trust and once you have left the Trust. This Privacy Notice explains how we collect, use, store, and share your personal data in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and other relevant data protection laws. Please read this notice carefully to understand how we manage your data.

Franklin College Trust is a provider, who is responsible for the collection and processing of your personal data, as defined by data protection laws. The Trust is the data controller and/or processor for personal data relating to you.

What Personal Data We Collect
We collect and process the following categories of personal data. The points below are only examples and not an exhaustive list, and may include other data where appropriate– if you have any questions, please contact the Data Protection Officer:

1. **Personal Information**: Name, address, date of birth, gender, contact details (including email and phone number), vehicle registration details.
2. **Characteristics**: Such as ethnicity, language, nationality, country of birth.
3. **Qualifications & Employment History Information**
4. **Attendance Information:** (such as number of absences and absence reasons).
5. **Special Educational Needs and Disabilities (SEND)**: If applicable, information about any special educational needs or disabilities if this has been disclosed to us.
6. **Emergency Contact Information**: Name and contact details of an emergency contact / next of kin.
7. **Financial Information**: relevant to payroll and pensions.
8. **Health and Wellbeing Data**: Any medical or health information or health needs you may have disclosed to us.
9. **Photographs and Video**: Photographs, videos or testimonials for example, during Trust activities or Trust related events for marketing or educational purposes. Including photograph of staff ID badge. These may all be used for promotional purposes and such as but not limited to, Trust printed publications, on the Trust website and on social media or any other suitable forum the Trust deems acceptable. Additionally, this information may be shared with schools, employers and any other appropriate third parties. These may also be used once you have left the Trust.
10. **HR Information:** such as Performance Management Reviews (PMR) and disciplinary matters.
11. **Recruitment Data:** (such as. interview notes, candidate selection)
12. **Criminal Convictions:** as part of the DBS and in accordance with the Rehabilitation of the Offenders Act (1974) and any other relevant legislation
13. **Legal requirements:** (such as Single Central Register, for compliance with KCSIE guidance)
14. **Management Information System:** any information that the staff member has recorded onto the internal system.
15. **Any other relevant data that the Trust deems appropriate**.

How We Use Your Personal Data
We use your personal data for the following purposes. The points below are only examples and not an exhaustive list, and may include other usages of your data where appropriate – if you have any questions, please contact the Data Protection Officer:

1. **To Provide Educational Services:** To allow staff to perform their duties within the Trust.
2. **To Monitor Progress and Achievement:** To assess the quality of our services and your progress and performance in your role

3. **To Provide Health and Welfare Support**: To provide appropriate support, care and guidance including in the event of an emergency or if you require any special assistance.
4. **To Manage Attendance**: To track and monitor your attendance at Trust.
5. **To Communicate with You:** To send you important information in order for you to fulfil your role.
6. **To Comply with Legal Obligations**: To meet legal and statutory requirements such as safeguarding, SEND, health and safety, and financial auditing and comply with the law regarding data sharing.
7. To ensure we meet all statutory employment requirements
8. To safeguard students and others
9. To fulfil payroll and pension obligations and provide information to appropriate third parties

The Trust will use the information provided in a manner that conforms with the Data Protection Act 2018 (DPA 2018), the UK GDPR and the Human Rights Act 1998.

We do not undertake any automated decision making. The Trust is committed to being transparent about how it collects, uses, stores and deletes data and to meeting its data protection obligations.

Why does the Trust collect and use staff information?
The Trust collects and uses staff information. The lawful basis on which we use this information is that we collect it as part of our public interest task of providing education to you. We collect and use staff information under Article 6 (1). of the UK General Data Protection Regulation 2018 (GDPR) where:
• To fulfil the contract each member of staff signs with the Trust upon employment
• Processing is necessary for compliance with a legal obligation to which the controller is subject
• Processing is necessary in order to protect the vital interests of the data subject
• Processing is necessary in order for us to carry out a public task
• Legitimate interests

We also collect and use staff information which is defined as a special category of personal data under Article 9 (2). of the GDPR 2018, such as biometric and ethnicity data. We also define other sensitive data as a special category, (this list is not exhaustive) for example SEND data.

• Processing is necessary for the purpose of carrying out obligations under employment and social security and social protection law.

• We are also required to share data with the Department for Education (DfE) about staff, e.g. the workforce survey / census.

Lawful Basis for Processing Your Personal Data
We rely on the following lawful bases to process your personal data. The points below are not an exhaustive list, and may include other lawful basis for processing your personal data where appropriate – if you have any questions, please contact the Data Protection Officer:

1. **Performance of a Contract**: The processing of your data is necessary to fulfil our contract with you.
2. **Legal Obligation**: We may process your data to comply with legal obligations.
3. **Consent**: In some cases, we may ask for your consent.
4. **Legitimate Interests**: We may process your data for legitimate interests, such as improving services and communications.

Your Rights

Under data protection law, you have the following rights regarding your personal data:
1. **Access**: You have the right to request access to the personal data we hold about you in certain circumstances.

2. **Rectification**: You have the right to request that we correct any inaccurate or incomplete data in certain circumstances.
3. **Erasure**: You have the right to request the deletion of your personal data in certain circumstances.
4. **Restriction**: You have the right to request that we restrict the processing of your personal data in certain circumstances.
5. **Data Portability**: You have the right to request that we transfer your personal data to another organisation.
6. **Objection**: You have the right to object to certain types of processing of your data in certain circumstances for example if it is likely to cause, or is causing, damage or distress.
7. **Withdrawal of Consent**: If we process your data based on your consent, you have the right to withdraw that consent at any time in certain circumstances.

You also have the right to:

- Object to processing of personal data that is likely to cause, or is causing, damage or distress
- Prevent processing for the purpose of direct marketing
- Object to decisions being taken by automated means
- In certain circumstance, have inaccurate personal data rectified, blocked, erased or destroyed

To exercise any of these rights, please contact the Trust's Data Protection Officer (DPO).

Right to request access to your information

Under data protection legislation staff have the right to request access to information about them that the Trust holds. To make a request for this, please email information.governance@franklin.ac.uk who will process the request in partnership with Franklin College Trust's Data Protection Officer.

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance to information.governance@franklin.ac.uk. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/make-a-complaint

Collecting staff information

Whilst the majority of staff information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain staff information to us or if you have a choice in this.

Raising a Data Protection Complaint – (Collecting, Using, Storing or Sharing Personal Data)

Individuals have the right to raise a complaint about how the Trust collects, uses, stores or shares personal data. The Trust will handle all data protection complaints in accordance with the requirements of the Data (Use and Access) Act 2025 and guidance issued by the Information Commissioner's Office (ICO).

Complaints can be submitted through the Trust to any of the following ways:

- Data Protection Officer (DPO)
- Email: information.governance@franklin.ac.uk
- Postal Address: [Data Protection Officer, Franklin College Trust, Chelmsford Avenue, Grimsby, DN34 5BY]

Data Protection Complaint Handling Process

- The Trust will provide individuals with clear and accessible ways to make a data protection complaint (as identified above).
- All complaints will be acknowledged within 30 calendar days of receipt.
- The Trust will investigate complaints without undue delay and make appropriate enquiries to establish the relevant facts.
- Individuals will be kept informed of the progress of their complaint and any significant developments during the investigation.

- Where necessary, the Trust will take corrective action to address identified issues or breaches.
- The Trust will communicate the outcome of the complaint to the individual without undue delay, including details of any actions taken.
- If an individual remains dissatisfied, they will be informed of their right to raise the matter with the Information Commissioner's Office (ICO).

CCTV

CCTV recordings are used and retained for a limited period to ensure the safety of student applicants, students, parents/guardians, staff and visitors to the Trust. Access to view and monitor these recordings is limited to the appropriate staff who will report and act accordingly if suspicious or inappropriate actions or behaviours are identified. CCTV images may be passed on to the police for the purposes of crime detection or prevention, and Franklin College Trust will also disclose CCTV footage when requested by insurance companies. CCTV may be used to assure the integrity of our examination arrangements, with footage shared with Awarding Organisations for audit and fraud prevention purposes.

How We Store Your Data

Your personal data will be stored securely and only for as long as necessary to fulfil the purposes for which it was collected, or as required by law. We implement appropriate technical and organisational measures to protect your data from loss, misuse, or unauthorised access.

Who We Share Your Data With

We may share your data with the following parties as required. The points below are not an exhaustive list, and may include other parties of who we share your data with, where appropriate – if you have any questions, please contact the Data Protection Officer:

1. **Internal Staff**: Trust staff involved in services that have an impact on your role and if our Trust policies allow it.
2. **Third-Party Providers**: External organisations that provide educational or administrative services, such as the Joint Council of Qualifications (JCQ), Lloyds Bank PLC, examination boards, online training providers, Evolve, Microsoft, Google, First Media Ltd, PPP Marketing Ltd, data analysis providers or IT support.
3. **We routinely share your information with Data Processors who enable the Trust to provide services:** such as ALPS, Sixth Sense Analytics, MIDES, UniFrog.
4. **Regulatory Authorities**: Relevant educational authorities, including the Department for Education (DfE), or Ofsted, for reporting and compliance purposes and Local Authorities.
5. **Health and Emergency Services**: In the event of an emergency, we may share relevant information with emergency services or health, well-being and safeguarding professionals and services including Social Services and the Police.
6. **Legal or Regulatory Bodies**: If required by law or to protect our legal rights, we may share your data with authorities, such as the police or a court of law.
7. **We occasionally share staff information with:** Civica (record system), Auditors, Insurers or other appropriate consultants.

We also routinely share staff data with the following parties as required. The points below are not an exhaustive list, and may include other parties of who we share your data with, where appropriate – if you have any questions, please contact the Data Protection Officer:

- Disclosure and Barring Service (DBS)
- East Riding Yorkshire Council (Payrolls & Pensions)
- Teachers, Pension Scheme.

These providers are classed as 'data processors' and are contractually obliged to keep your details secure and use them only to provide particular services to you or the Trust in accordance with our instructions.

Privacy Notice – Staff

We also routinely share staff data with the following parties as required. The points below are not an exhaustive list, and may include other parties of who we share your data with, where appropriate – if you have any questions, please contact the Data Protection Officer:

- RCU
- Police / Emergency Services
- Cull Micro Imagining (scanning bureau)
- Department for Education
- Edenred Childcare vouchers
- Cyclescheme
- RSM Auditors
- Screencast-o-matic (Content Creation Website)
- GroFar Software (Careers & Work Placement Software)

We are also required to share information about our employees with the Disclosure Barring Service (DBS).

DBS Personal Information Charter: Personal information charter - Disclosure and Barring Service - GOV.UK
Before sharing your data with a party, we will either obtain your consent or establish that the sharing is necessary (which includes ensuring that the data shared is kept to a minimum), fair and otherwise within the law.

We will not pass your information to third parties for them to contact you directly for their own marketing purposes.

Occasionally information will be shared with the department for education. For more information about the department's data sharing process please visit: How DfE shares personal data - GOV.UK

How to Contact Us
If you have any questions or concerns about how we process your personal data, please contact:
Data Protection Officer
Email: information.governance@franklin.ac.uk
Telephone number: 01472 875000

Changes to This Notice
This Privacy Notice is subject to change. We may update this Privacy Notice from time to time to reflect changes in our practices or legal requirements.