

How we use student information?

Date: Nov 2024

Review Date: Nov 2025

Version: 1

Document owner: Fir Tree College

A: The Nook, Appley Bridge, Wigan, WN6 9JB

T: 01257 251 502 | E: info@firtreecollege.com



Introduction

Fir Tree College must process the personal data of those that enrol with us as students. We need information about our students and their families to support each learner through their qualifications and ensure that we provide a safe and secure environment for learning and development.

As part of our obligations under the UK General Data Protection Regulation (UK-GDPR) we must inform individuals:

- What personal data we collect about them
- How and why we use that personal data
- What their rights are under data protection law
- How to contact us to exercise those rights

We do this by providing privacy notices. A summarised version of this document is available on our website.

Data Controller

The college is the 'Data Controller' for the personal information that we process about students and their families. This means that we are responsible for this data and make decisions on how it is used.

Data Protection Officer

The college has appointed a Data Protection Officer (DPO) who is responsible for overseeing compliance with the relevant data protection legislation. Our DPO provides support to the college and acts as the first point of contact for any questions or queries regarding data protection.

Our DPO is Miss Danielle Eadie from RADCaT Ltd who is supported by Senior Leadership Team (SLT) at the college. The DPO is contactable via the college office in the first instance.

The categories of student information that we collect and process:

Activity	Categories of data	Source
Application & enrolment	<ul style="list-style-type: none">- Full name- D.O.B- Address & contact details- Educational history & qualifications- Special educational needs*- Parent or guardian names & contact details- Emergency contacts	<p>Direct: completion of admissions pack</p> <p>Note: referrals may be received from local authority or previous school</p>

	- Bank account details (funding & benefit payments)	
Equalities monitoring	- Age - Gender* - Ethnicity* - Nationality (language etc)* - Special educational needs (disabilities, medical conditions etc)* - Reasonable adjustments required	Direct: completion of admissions pack Note: referrals may be received from local authority or previous school
Educational	- Courses - Progress & development - Grades & qualifications - Reports	Collated by the college; results and certifications provided by awarding body
Pastoral:	- Attendance & absences - Behaviour logs - Safeguarding records* - Special educational needs (SEN) records*	Collated by the college; in respect of safeguarding and SEN records, data may be received from external sources, support agencies etc
Operations:	- Images (promotional) - Images (CCTV) - Voice recordings (CCTV) - Usage data (systems and email etc) - Accident & incident records*	Collated by the college

***Special Category Data**

Why we collect and use student information:

- to support student learning
- to keep students and other members of the college community safe from harm
- to monitor and report on student attainment progress.
- to provide appropriate pastoral care
- to assess the quality of our services
- to meet the statutory duties placed upon us by the DfE and other governing bodies
- to celebrate achievements and give the community an insight into college life

The lawful basis for processing personal data

Data protection law requires us to meet at least one of the following lawful bases to process personal data:

- There is a **legal obligation** to process personal data
- There is a **contractual obligation** to process personal data
- Personal data is processed in the performance of a **public task** (task: laid down in law)
- There is a **vital interest** to process personal data
- There is a **legitimate interest** to process personal data
- The individual has provided their **consent** to process their personal data

For the most part, the college process student data to fulfil a **legal obligation** or **public task** that is laid down in law, namely:

- Education Act (1996)
- Equality Act (2010)
- Further & Higher Education Act (1992)
- Health & Safety at Work Act (1974)
- Keeping Children Safe in Education (2024)
- Safeguarding Vulnerable Groups Act (2006)
- Special Educational Needs & Disability (SEND) Regulations (2024)
- DfE & ESFA Statutory Data Collections

***Please contact the college office if further information is required about our legal obligations.**

In certain circumstances we will also rely upon the following lawful bases:

- **Vital interests:** if an incident or accident occurs and we must process personal data in the act of protecting or saving someone's life.
- **Consent:** in situations where the processing of personal data is optional, for instance inclusion in images for the college's social media pages.

Special category data

Special category data is information that we process that is much more sensitive in nature such as details about health and wellbeing and characteristics including gender and ethnicity. The college must take extra measures to ensure such information is secure and confidential, therefore we must meet an additional lawful basis from the UK-GDPR.

When processing special categories of personal data in the routine running of the college, we rely upon the following conditions:

1. The individual has provided **explicit consent** (written) for instance if we would like to make a referral to an outside agency for support with their health and wellbeing; this will typically involve the sharing of student records containing health information.
2. Personal data is processed for reasons of **substantial public interest** including:
 - Sharing special categories of personal data about students with the government to meet our legal and statutory obligations; submitting census data to the DfE for instance.
 - Collecting special categories of personal data for equal opportunities monitoring to ensure all of our students receive equal treatment.
 - Referring serious safeguarding concerns about a student's health and wellbeing to the police and social services; in situations where consent is not appropriate.
3. The college must process special category data in the act of protecting or saving someone's life; there is a **vital interest**. We have a duty to inform emergency services of any known allergies or medical conditions if an accident occurs.

In certain circumstances, the college may be required to process personal data (including special category) for the following reasons:

- If the college is involved in a legal claim that involves a student or their family; in such instances, we are processing personal data as part of or in defence of **legal claims and other judicial acts**.

- The college may be instructed to partake in public vaccination programs and health monitoring in situations where there is a threat to health such as a pandemic. In such instances, our lawful basis to process student health records is for **reasons of public interest in the area of public health.**

CCTV

CCTV is in place in and around the college site. Cameras are located internally and externally with some recording both images and sound. We use CCTV for the following purposes:

- Keep our premises and members of the college community and wider public safe from harm
- Prevent and detect crime and assist in apprehending offenders where necessary
- Review and evidence any instances of inappropriate behaviour by staff, students and other visitors to site

We do not routinely monitor the footage and will only access the recordings if we are notified of an incident.

System Monitoring

If students are provided with access to devices and digital systems as part of their course, automated usage logs will be recorded as standard. Whilst we do not monitor usage on a routine basis, we will review such information if we have cause for concern or are notified of any inappropriate use that may put our systems or people at risk.

How we keep your data secure?

Records held in electronic format are stored securely on carefully selected databases and systems that are fully encrypted; two factor authentication utilised where available. Physical records are kept in locked cabinets within locked offices and archive rooms. Access to records is strictly limited on a need to know basis; all staff are subject to vetting checks and confidentiality agreements.

If we must transfer data to third parties, we will ensure this is done so using secure transfer methods.

Storing and retaining student data

To comply with the UK-GDPR, the college only keep personal data for as long as necessary to meet our legal and operational duties. As a rule of thumb, student records are kept securely for up to 6years from the date they leave.

Who we share student information with and why?

We will only share student information if it is required by law or for operational purposes; we will seek consent for data sharing in situations where the sharing of data is optional.

By law, we must share data with the following parties:

- The Local Authority: the Education Act (1996) poses obligations on local authorities to support and monitor education and training for children and young people.
- Department for Education (DfE): requires the statutory sharing of student information; data underpins funding and decision making.

Student data will also be shared with the awarding bodies that accredit the courses that we deliver and provide certificates and qualifications. This is currently limited to Pearson (Edexcel).

We also appoint a number of external service providers that help to ensure the college runs smoothly and is compliant with the law. These include:

- ICT provider (student access to college systems)
- Information management systems (manage student records more effectively)
- Educational resource providers (apps and learning software, specialist tutors etc)
- Health and wellbeing support providers (therapists, health & social workers etc)

In certain circumstances, we **may** be required to share student data with the following parties usually if an accident or incident has occurred:

- Police and emergency services
- Social workers and other support authorities
- Professional advisors (solicitors etc)
- Insurance (claims etc)
- Courts (legal claims)
- Regulatory and supervisory authorities (HSE, ICO, Ofsted, DfE)

We take a minimalist approach to data sharing; we will only disclose what is strictly necessary to fulfil the purpose of the data sharing. Checks are performed on service providers that process data on our behalf to ensure that they are compliant and possess good technical and organisational security standards.

Transferring data internationally

We do not routinely transfer the personal data of students and their families outside of the United Kingdom (UK). In the event that we must do so, we will ensure that any transfer is compliant and the relevant safeguards are in place.

What are your rights?

All individuals have the following rights in respect of their own personal data in certain circumstances:

- The right to be informed about how and why we process your personal data
- The right to access and ask for copies of the personal data we hold about you
- The right to ask that we rectify any personal data you feel is inaccurate or incomplete
- The right to object to the processing of your personal data in certain circumstances
- The right to ask us to erase the personal data that we hold about you in certain circumstances
- The right to ask us to restrict the processing of your personal data
- The right to ask that we transfer your personal to another controller via automated means (data portability)
- The right to ask that your personal data is not subject to automated decision making and profiling

Who can make a request?

Student personal data belongs to the student and not their parent or guardian. However, we realise that some students may have vulnerabilities that may impact their ability to understand and make informed decisions about their own data. In such cases, we will seek input from the parent or guardian

if we receive a request relating to a student's rights. Similarly, we may need to seek approval from the student if a request is received from their parent or guardian or another third party.

How to make a request:

We ask that all requests are sent to the college office and addressed to the 'Data Protection Officer' (DPO). Please note that we may need to verify your identity with copy identification and further documentation if the requester is not known to us.

A response will be provided within one calendar month; we reserve the right to extend more complex requests by a further two calendar months. We will inform the requester of any intention to extend within the first month.

Our 'Data Protection Policy' is available on our website and provides further details on rights.

Complaints

If you have any concerns about how and why we process your personal data, please contact us in the first instance so that we can resolve any issues accordingly.

You can also complain to the Information Commissioners Office (ICO) if you are unhappy with how we have used your data:

ICO: <https://ico.org.uk/make-a-complaint/data-protection-complaints/>