

Privacy and Data Protection Notice

Version Date:	September 2025
Signed:	Principal
Signed:	Chair of Governors
Review cycle:	1 year
Date of next review:	September 2026

Contents

1. Introduction	3
2. Our approach to data protection	3
3. The personal data we hold	4
4. Why we use this data	5
5. Our lawful bases for using this data	6
6. Collecting this data	7
7. How we store this data	7
8. Who we share data with	7
9. Transferring data internationally	8
10. Photographs and media	9
11. CCTV	9
12. Your rights regarding personal data	9
13. Complaints about data protection	10
14. Cybersecurity and data security	11
15. Contact us	11
16. Changes to this notice	11

1. Introduction

Under UK data protection law – the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025 – 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 this Privacy Notice (sometimes called a ‘fair processing notice’).

This Privacy Notice explains how we collect, store and use personal data about:

- Pupils, and prospective pupils and their families during the admissions process
- Parents and carers, and educational guardians of our pupils
- Staff (the school workforce) and job applicants
- Governors and volunteers
- Visitors to the school site
- Suppliers and service providers (their staff and representatives)

Where this notice refers to ‘you’, this means the individual whose data we are processing; for younger pupils who are not yet able to understand and exercise their own data protection rights (generally considered to be under age 12, assessed case by case), parents/carers may exercise these rights on their child’s behalf.

Felixstowe International College, Maybush House, Maybush Lane, Felixstowe, Suffolk, IP11 7NA, is the ‘data controller’ for the purposes of UK data protection law. This means we are responsible for deciding how we hold and use personal information about you.

This notice replaces all previous versions and is approved by the Data Privacy Lead: Cerys Parker. A summary of changes is given in the document history in section 16.

2. Our approach to data protection

As an independent school, Felixstowe International College is not legally required to appoint a formally designated Data Protection Officer (DPO) under Article 37 of the UK GDPR. In line with guidance from the Independent Schools Association (ISA), we do not use the title ‘DPO’, as doing so creates additional statutory obligations that are not proportionate to our setting.

Instead, we take a whole-school approach to data protection compliance, led by a designated member of staff with the title Data Privacy Lead. The Data Privacy Lead is responsible for:

- Overseeing day-to-day compliance with data protection law
- Maintaining this Privacy Notice and related policies
- Acting as the first point of contact for data protection queries, subject access requests, and complaints
- Liaising with the Information Commissioner’s Office (ICO) where required
- Ensuring all staff receive appropriate data protection and cybersecurity awareness training
- Maintaining records of processing activities

The Data Privacy Lead is independent of the systems used to manage and store personal data (e.g. Google Workspace), in line with best practice on separation of roles.

Contact details for the Data Privacy Lead: Cerys Parker – cerysparker@ficedu.org

The school also liaises with the Designated Safeguarding Lead (DSL), Chaerin Lee, on matters where data protection and safeguarding intersect, including the handling of sensitive personal data relating to child protection.

3. The personal data we hold

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

3.1 Pupils

- Contact details, contact preferences, date of birth, identification documents (including passports, visas and immigration status for pupils on the Child Student route)
- Results of internal assessments and externally set tests, and pupil and curricular records
- Characteristics, such as ethnic background, nationality, first language, or special educational needs (SEN)
- Exclusion and behaviour information
- Details of any medical conditions, including physical and mental health
- Attendance and boarding records
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Information about a pupil's use of our information and communication systems, equipment and facilities (e.g. school computers)
- Photographs and CCTV images captured in school

3.2 Parents, carers and educational guardians

- Names, contact details and contact preferences (including overseas addresses)
- Financial information, including bank details, for the administration of fees
- Details of parental responsibility, court orders and family circumstances where relevant to the care of your child
- Details of appointed educational guardians in the UK and, where relevant, education agents

3.3 Staff and job applicants

- Name, 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, cover letter or application form
- 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
- Information about criminal convictions and offences, including data received from the Disclosure and Barring Service (DBS), as part of our safer recruitment duties

- Information about use of our information and communication systems, equipment and facilities

3.4 Governors, volunteers, visitors and suppliers

- Names, contact details and, where required for safeguarding, identification and vetting information (including DBS checks for governors and regular volunteers)
- Registers of business and pecuniary interests for governors
- Visitor records (sign-in details, vehicle registration where applicable) and CCTV images
- For suppliers and their staff: contact details, bank and payment information, and contract records

3.5 Special category and criminal offence data

Some of the data above falls into ‘special categories’ of more sensitive personal data – including information about health (physical and mental), ethnic background, religious beliefs, and (for staff) trade union membership. We may also process information about criminal convictions and offences, principally in connection with safer recruitment and safeguarding. We give this data extra protection, as explained in section 5.

We may also hold data that we have received from other organisations, including other schools, local authorities, the Department for Education, education agents, and (in respect of criminal offence data) the Disclosure and Barring Service.

4. Why we use this data

We use this data to:

- Support pupil learning, and monitor and report on pupil progress
- Provide appropriate pastoral and boarding care, and protect pupil welfare
- Administer admissions, and sponsor and support pupils who require a visa to study in the UK
- Keep parents/carers and guardians informed about their child’s education and the running of the school, and process payment of fees
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Administer employment contracts, including enabling staff payment
- Enable governors and volunteers to carry out their roles, and meet our regulatory obligations
- Keep the school site safe and secure, including managing visitors
- Administer contracts with suppliers and service providers
- Assess the quality of our services and carry out research
- Make sure our information and communication systems, equipment and facilities are used appropriately, legally and safely
- Comply with the law regarding data sharing

We will only use personal information for the purposes for which we have collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use personal information for an unrelated purpose, we will notify you and explain the legal basis which allows us to do so. Please note that we may process personal information without your knowledge or consent, in compliance with these rules, where this is required or permitted by law.

4.1 Marketing

Where you have given us consent to do so, we may send you marketing information by email promoting school events, campaigns, charitable causes or services that may be of interest to you. You can withdraw consent or 'opt out' of receiving these communications at any time by using the 'unsubscribe' link at the bottom of any such communication, or by contacting the Data Privacy Lead.

4.2 Automated decision-making and profiling

We do not currently process any personal data through automated decision-making or profiling. If this changes in the future, we will amend this Privacy Notice to explain the processing to you, including your right to object to it.

4.3 Filtering and monitoring

While pupils are at our school, we may monitor their use of our information and communication systems, equipment and facilities (e.g. school computers). We do this so we can comply with our legal obligations (including our safeguarding duties under Keeping Children Safe in Education), comply with our policies (e.g. child protection policy and IT acceptable use policy), keep our networks and devices safe from unauthorised access and malicious software, and protect pupil welfare. Staff use of school systems may also be monitored for the same purposes.

5. Our lawful bases for using this data

We only collect and use personal data when the law allows us to. As an independent school, we most commonly process personal data where:

- **Contract** – we need to process data to fulfil a contract, most notably the parent contract for the provision of education and boarding, and employment contracts with staff and contracts with suppliers
- **Legal obligation** – we need to process data to comply with the law, for example our safeguarding duties, our duties as a sponsor of pupils on the Child Student visa route, health and safety law, and employment and tax law
- **Legitimate interests** – we have a legitimate interest in processing the data and there is minimal privacy impact, for example providing education and pastoral care effectively, promoting the school, preventing fraud, and ensuring network and information security

Less commonly, we may also process personal data where:

- **Consent** – we have obtained consent to use it in a certain way (for example, for certain photographs or marketing). Where we rely on consent, it can be withdrawn at any time; we will make this clear when we ask for consent and explain how to withdraw it
- **Vital interests** – we need to protect an individual's vital interests (or someone else's interests), for example in a medical emergency

Some of the purposes listed in section 4 overlap, and there may be several grounds which justify our use of the data.

5.1 Our basis for using special category data

For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in UK data protection law:

- We have obtained your explicit consent to use the data in a certain way

- We need to perform or exercise an obligation or right in relation to employment, social security or social protection law
- We need to protect an individual's vital interests (i.e. protect a life), in situations where the individual is physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for the establishment, exercise or defence of legal claims
- We need to process it for reasons of substantial public interest as defined in legislation (including safeguarding children)
- We need to process it for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional, or by any other person obliged to confidentiality under law

5.2 Our basis for using criminal offence data

For data about criminal convictions and offences, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in UK data protection law – most commonly that the processing is necessary for reasons of substantial public interest, such as safeguarding children through safer recruitment checks.

6. Collecting this data

While most of the information we collect 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.

Most of the data we hold will come from you, but we may also hold data received from other sources, including: other schools; education agents and educational guardians; local authorities; government departments or agencies (including the Home Office / UK Visas and Immigration); the Department for Education; examination boards; the Disclosure and Barring Service; and police forces, courts or tribunals.

7. How we store this data

We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary to comply with our legal obligations or regulatory requirements. We follow the Information and Records Management Society's Toolkit for Schools in determining appropriate retention periods. Details of retention periods for particular records are available from the Data Privacy Lead on request.

We take appropriate technical and organisational measures to protect personal data against unauthorised access, loss or destruction. This includes cybersecurity controls, staff training and access restrictions. Our approach to cybersecurity is documented separately in our Cybersecurity Awareness Plan and Cybersecurity Risk Assessment (see section 14).

We will dispose of personal data securely when we no longer have a legal requirement to retain it.

8. Who we share data with

We do not share personal information 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 UK data protection law), we may share personal information with:

- The Home Office / UK Visas and Immigration (UKVI) – to meet our legal duties as a licensed sponsor of international pupils on the Child Student route, including reporting on enrolment and attendance
- The Department for Education (DfE) – to meet our legal obligations as an independent school, including the annual school level census (SLASC) and registration requirements
- The pupil's family, representatives and appointed educational guardians – for the care of the pupil and in emergencies such as a health matter
- Education agents – where they act on behalf of a pupil's family in the admissions process
- Educators and examining bodies – necessary for the performance of our education function
- Our regulator, the Independent Schools Inspectorate (ISI) – to enable it to evaluate the education and boarding provision we provide
- Suppliers and service providers – to enable them to provide the service we have contracted them for (for example, IT and cloud services, catering, transport and educational platforms)
- Follow-on schools and other schools which a pupil attends after leaving us – to support continuity of education
- Our auditors and professional advisers – to meet our finance and legal obligations
- Health and social welfare organisations – to enable us to comply with our duty of care and statutory safeguarding duties. This may include therapists, clinical psychologists, CAMHS, school counsellors, social care and the Educational Welfare Office (EWO)
- Local authorities – to meet our legal obligations to share certain information, such as safeguarding concerns
- Professional bodies – necessary for the performance of our education function
- Police forces, courts and tribunals – in order to uphold law and order

8.1 National Pupil Database

Some pupil information – for example, information collected via statutory data collections and public examination results – is stored in the National Pupil Database (NPD), which is owned and managed by the DfE and provides evidence on school performance to inform research. The DfE may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data. For more information, see the DfE's webpage on how it collects and shares research data, or contact the DfE.

9. Transferring data internationally

Given our international pupil body, some data transfers occur across borders – for example, communicating with parents/carers and agents overseas, or using cloud services with servers outside the UK. Where we transfer personal data to a country or territory outside the United Kingdom, we will do so in accordance with UK data protection law: either the UK government has made 'adequacy regulations' in respect of the destination country, or we will put appropriate safeguards in place (such as the International Data Transfer Agreement or Addendum). You can obtain a copy of any such safeguards by contacting the Data Privacy Lead.

10. Photographs and media

As part of our activities, we may take photographs and allow external organisations to take photographs or to film within our school. You will be made aware when this is happening and the context in which the photograph will be used.

We will take photographs for use by the school. Usually these will be unnamed and will generally be for internal school use, but may also include photographs for publications such as:

- Photographs included in the school's prospectus
- Photographs to be used on display boards which can be seen by visitors to the school
- Photographs posted on the school's official social media sites and its own website. Such sites can be accessed by the public and will therefore require close monitoring by school staff to ensure they are appropriate

Named photographs will be used for internal use where there is a clear lawful basis for doing so – for example, for identifying pupils for medical or safeguarding requirements. For all other purposes, consent will be sought from parents/carers (or from pupils themselves where they are able to give it).

11. CCTV

The school operates CCTV on its premises. This is considered necessary to protect the safety of staff, pupils and visitors, and the property of the school. CCTV footage is retained only as long as necessary and is held securely. We follow the ICO's guidance on video surveillance.

12. Your rights regarding personal data

12.1 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.

Parents and 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 (generally under the age of 12, considered case by case), or where the child has provided consent.

If you make a subject access request, and if we do hold information about you or your child, we will (subject to any exemptions that apply):

- 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
- Tell you about your right to complain to us (see section 13) and to the ICO
- 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. To make a subject access request, please contact the Data Privacy Lead.

12.2 Other rights

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 personal data 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 (rectification), deleted or destroyed (erasure), or restrict processing
- Withdraw consent, where processing is based on consent
- Claim compensation for damages caused by a breach of data protection law

To exercise any of these rights, please contact the Data Privacy Lead.

13. Complaints about data protection

13.1 General data protection complaints

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 by contacting the Data Privacy Lead.

13.2 Formal data protection complaints procedure (section 164A)

From 19 June 2026, section 164A of the Data Protection Act 2018 (inserted by section 103 of the Data (Use and Access) Act 2025) requires the school, as a data controller, to operate a formal complaints procedure for data subjects. Individuals should make a formal complaint to the school before approaching the ICO. This procedure is integrated into our existing school complaints policy (ISS Standard 33) in accordance with ICO guidance.

The following procedure applies to any person (parent, pupil, member of staff or other individual) who believes their personal data has been handled incorrectly by the school.

Step 1 – Informal stage. Contact the Data Privacy Lead in the first instance. We aim to acknowledge your concern within five working days and resolve it informally where possible. Many concerns can be resolved at this stage without the need for a formal complaint.

Step 2 – Formal written complaint. If you are not satisfied with the informal response, you may submit a formal written complaint to the Data Privacy Lead – electronically using the school office email address or by post. Please set out your name and contact details, the nature of the data protection concern, and what outcome you are seeking. We will acknowledge receipt of your formal complaint in writing within 30 calendar days of receiving it, in accordance with section 164A of the Data Protection Act 2018. We will investigate your complaint without undue delay, keep you informed of progress, and communicate the outcome to you in writing once the investigation is complete.

Step 3 – Panel hearing. If you remain dissatisfied following the formal written stage, the matter may proceed to a panel hearing in line with the school's complaints policy under ISS Standard 33. Details of this process are set out in the school's full Complaints Policy, which is available on the school website and on request.

Record-keeping. The school keeps a written record of all formal data protection complaints, the steps taken to investigate them, and any actions taken as a result, regardless of outcome. Records are held confidentially and are available to the Secretary of State and inspection bodies where required.

13.3 Right to escalate to the ICO

If you remain dissatisfied after completing our complaints procedure, you have the right to complain to the Information Commissioner's Office (ICO):

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

Under section 164A of the Data Protection Act 2018 (in force 19 June 2026), individuals are expected to raise concerns with the school first, before contacting the ICO. The ICO may take into account whether our complaints procedure has been followed when considering any complaint.

14. Cybersecurity and data security

Felixstowe International College takes the security of personal data seriously. We maintain a Cybersecurity Awareness Plan and a Cybersecurity Risk Assessment, which are reviewed annually and are available to staff and relevant stakeholders.

All staff are required to complete cybersecurity awareness training. This training covers:

- Recognising phishing and social engineering threats
- Safe handling of personal data
- Password security and access control
- Reporting suspected security incidents

Any actual or suspected personal data breach must be reported to the Data Privacy Lead immediately. Where a breach is likely to result in a risk to individuals' rights and freedoms, we will notify the ICO within 72 hours in accordance with Article 33 of the UK GDPR, and will inform affected individuals where the risk is high.

15. Contact us

If you have any questions, concerns or would like more information about anything mentioned in this Privacy Notice, please contact our Data Privacy Lead:

Cerys Parker – Data Privacy Lead, Felixstowe International College – cerysparker@ficedu.org

You may also write to us at: Felixstowe International College, Maybush House, Maybush Lane, Felixstowe, Suffolk, IP11 7NA.

16. Changes to this notice

We may update this Privacy Notice from time to time. Any significant changes will be communicated to parents, pupils and staff. The current version is always available on the school website.

Document history:

- Version 1.0 – Original notice (external DPO model, Andy Crow / DPO for Education)

- Version 2.0 – 15 June 2026: Removal of external DPO; introduction of internal Data Privacy Lead; addition of s.164A complaints procedure; cybersecurity section added; updated to reflect Data (Use and Access) Act 2025
- Version 3.0 – September 2026: Notice extended to cover all data subjects (pupils, parents/carers and guardians, staff, job applicants, governors and volunteers, visitors, suppliers), cross-referenced against The Key's model privacy notices (Dec 2024). New sections on special category and criminal offence data conditions, marketing, automated decision-making, filtering and monitoring, and sources of data. Lawful bases restated for an independent school (contract, legal obligation, legitimate interests, consent, vital interests). Data sharing updated (UKVI/Home Office sponsor duties, SLASC, guardians and agents). Electronic complaint form route added to s.164A procedure. Address corrected.