

Privacy and Data Protection Notice

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

1. Introduction

Under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025

*This notice replaces all previous versions and is **approved by the Data Privacy Lead: Cerys Parker**. The key changes from version 1 are: (a) removal of reference to an external Data Protection Officer; (b) introduction of an internal Data Privacy Lead; (c) new data protection complaints procedure under section 164A of the Data Protection Act 2018, in force 19 June 2026; and (d) updated cybersecurity acknowledgement.*

Under the UK GDPR and the Data Protection Act 2018, 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') to individuals where we are processing their personal data.

This Privacy Notice explains how we collect, store and use personal data about pupils, parents and staff.

Felixstowe International College is the 'data controller' for the purposes of data protection law. This means we are responsible for deciding how we hold and use personal information about you.

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 / G Suite), in line with best practice on separation of roles.

Contact details for the Data Privacy Lead:

- Cerys Parker — Data Privacy Lead
- 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) about pupils, parents and staff includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Bank account details, payroll records, National Insurance number and tax status information
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, 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

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

4. Why We Use This Data

We use this data to:

- Support pupil learning
 - Monitor and report on pupil progress
 - Provide appropriate pastoral care
 - Protect pupil welfare
 - Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
 - Enable staff payment
 - Carry out research
 - Comply with the law regarding data sharing
-

5. Our Legal Basis for Using This Data

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

- We need to comply with a legal obligation
- We need to fulfil a contract with you
- We need to carry out a task in the public interest

Less commonly, we may also process 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)
- We have legitimate interests in processing the data — for example, fraud prevention or ensuring network and information security

Where we have obtained consent to use 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 personal data overlap, and there may be several grounds which justify our use of this data.

6. Collecting This Information

While most of the information we collect about pupils 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.

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.

We follow the Information and Records Management Society's Toolkit for schools in determining appropriate retention periods.

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.

8. Data Sharing

We do not share information about pupils 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 pupils with:

- Border Agency
- The Department for Education — to meet our legal obligations as part of data collections such as the School Census
- The pupil's family and representatives — in case of emergencies such as a health matter
- Educators and examining bodies — necessary for the performance of our education function
- Our regulator, Independent Schools Inspectorate (ISI) — to enable it to evaluate the education we provide to your child, which is in the public interest
- Suppliers and service providers — to enable them to provide the service we have contracted them for
- Follow-on schools and other schools — which your child attends after leaving their current school, in the public interest of delivering education
- Our auditors — to meet our finance obligations as part of a statutory requirement, i.e. Annual Report and Accounts
- Health and social welfare organisations and third parties — to enable us to comply with our duty of care and statutory safeguarding duties for your child's welfare. This may include therapists, clinical psychologists, CAMHS, school counsellors, social care, and the Educational Welfare Office (EWO)
- Professional bodies — necessary for the performance of our education function
- Police forces, courts, tribunals — in order to uphold law and order

9. National Pupil Database

We are required to provide information about pupils 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 Pupil Database (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research. The Department for Education 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 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.

10. Transferring Data Internationally

Given our international student body, we recognise that some data transfers may occur across borders. Where we transfer personal data to a country or territory outside the United Kingdom, we will do so in accordance with Data Protection Law and will ensure appropriate safeguards are in place.

11. 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.

12. CCTV

The school operates CCTV on its premises. This is considered necessary to protect staff and pupils' safety and the property of the School. CCTV footage is retained only as long as necessary and is held securely.

13. Parents' and Pupils' Rights Regarding Personal Data

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 (usually under the age of 12), 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:

- 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.

To make a subject access request, please contact the Data Privacy Lead.

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 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 the Data Privacy Lead.

14. Complaints About Data Protection

14.1 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.

14.2 Formal Data Protection Complaints Procedure (from 19 June 2026)

Important — new statutory requirement: 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 schools, as data controllers, 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. Please set out:

- Your name and contact details
- The nature of the data protection concern
- 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 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.

14.3 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/concerns/>
- 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.

15. 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.

16. 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 Land
Felixstowe
Suffolk
IP11 7NA

17. 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
-