



Privacy Notice – Secondary Schools

Introduction

We are Plymouth CAST Multi Academy Trust. We are a Multi-Academy Trust of 34 schools and one nursery, for mixed pupils aged from three months to 18 years old. The schools within our Trust can be viewed on our Trust [website](#).

Our registered address is Edmund Rice Building, 21 Boniface Lane, Manadon Park, Plymouth, PL5 3AG.

This Privacy Notice is for our Plymouth CAST Secondary Schools.

We are the data controller for the personal information we process and are responsible for ensuring that it is handled lawfully, fairly and securely. Our Data Protection Registration Number is ZA022556.

This notice explains:

1. How we collect personal information
2. What personal information we collect and why
3. Use of CCTV
4. Use of Artificial Intelligence (AI)
5. Who we share information with
6. Our lawful bases for processing
7. How we keep information secure
8. How long we keep information
9. International transfers
10. Your data protection rights
11. How to contact us or make a complaint

1. How we collect personal information

We collect personal information directly from individuals when, for example, you:

- register a child with the school
- provide information during a pupil's education
- apply for employment, volunteering or a governor role
- work for or provide services to the school
- visit our premises, website or use our systems
- make an enquiry, request or complaint

We may also receive information from other organisations or individuals, including:

- previous or future schools
- parents and carers
- local authorities and the Department for Education
- health, social care and safeguarding professionals
- the police, courts and other public authorities
- employers, referees and recruitment suppliers
- contractors and service providers.



2. What personal information we collect and why

Students

We may collect:

- identification and contact details, including name, date of birth, address, Unique Pupil Number, , student account details and examination or candidate number
- biometric identifiers, such as fingerprints or facial recognition data where the school uses biometric systems
- characteristics such as sex, ethnicity, nationality, language, free school meal eligibility and looked-after status
- education records including attainment, progress, assessments and reports
- attendance and punctuality records
- behaviour, exclusions, pastoral and welfare information
- safeguarding concerns, referrals and interventions
- Special Educational Needs and Disabilities (SEND) information, including Education, Health and Care Plans;
- health, medical, disability, allergy, dietary and first-aid information
- relevant family circumstances and court orders
- religious or philosophical beliefs where relevant
- photographs, video recordings, online meeting recordings, transcripts and CCTV footage
- consents and permissions
- careers, work experience and destination information, including post-16 or post-18 education, training and employment plans
- information about the use of our school systems, networks and school-managed devices, including filtering and monitoring information
- online learning information, including account details, assignments or work submitted, teacher feedback, progress information and relevant platform activity

We use this information to provide education and pastoral support, deliver and manage online learning, monitor pupils' progress, safeguard pupils, manage attendance and behaviour, support SEND and health needs, administer admissions, communicate with families, monitor equality and meet our legal and statutory obligations.

Parents and carers

We may collect:

- name and contact details
- parental responsibility and family relationship information
- relevant family circumstances, court orders and safeguarding information
- payment and financial information
- eligibility information relating to benefits or financial support
- religious or philosophical beliefs where relevant to admissions or school activities
- consents and permissions
- images and visitor records



We use this information to communicate with families, administer pupils' education and welfare, manage admissions and payments, meet safeguarding responsibilities and comply with legal and reporting requirements.

Employees

We may collect:

- identification, contact and emergency contact information
- employment, contractual and payroll records
- bank, tax, National Insurance and pension information
- qualifications, professional registrations and training records
- recruitment and safer recruitment information
- Disclosure and Barring Service and other statutory check information
- attendance, absence, performance, disciplinary and grievance records
- health, disability and occupational health information
- equality monitoring information
- religious or philosophical beliefs and trade union membership where relevant
- photographs, video recordings, online meeting recordings, transcripts and CCTV footage
- information about the use of our school systems, networks and school-managed devices, including filtering and monitoring information

We use this information to recruit and employ staff, administer contracts and payroll, fulfil safeguarding and employment obligations, manage performance and attendance, provide reasonable adjustments and meet our legal and regulatory responsibilities.

Temporary workers, contractors and trainee teachers

We may collect:

- identification and contact details
- qualifications, recruitment and safeguarding checks
- contract and payment information
- health and disability information
- attendance records and images
- photographs, video recordings, online meeting recordings, transcripts and CCTV footage
- information about the use of our school systems, networks and school-managed devices, including filtering and monitoring information

We use this information to confirm suitability, manage contractual arrangements, safeguard pupils, make payments and comply with legal and regulatory requirements.

Governors and trustees

We may collect:

- identification and contact details
- appointment and term-of-office information
- committee memberships and attendance records
- declarations of interests
- statutory eligibility, DBS and Section 128 checks where applicable
- equality, health and disability information
- religious or philosophical beliefs where relevant



- photographs, visitor records, online meeting recordings, transcripts and CCTV footage
- information about the use of our school systems, networks or school-managed devices, where applicable

We use this information to administer governance, confirm eligibility and suitability, manage conflicts of interest and comply with statutory governance requirements.

Volunteers

We may collect:

- identification and contact details
- DBS or safeguarding checks
- training and qualifications
- volunteering records
- health and disability information
- photographs, CCTV footage and visitor records

We use this information to confirm suitability, manage volunteering arrangements and meet our safeguarding responsibilities.

Job applicants

We may collect:

- identification and contact details
- application forms and personal statements
- employment history and reasons for leaving previous roles
- qualifications, skills and training
- referee details and references
- right-to-work documentation
- criminal record and safer recruitment declarations
- information obtained through proportionate online searches of shortlisted applicants
- CCTV footage and visitor records

We use this information to assess suitability for employment, carry out safer recruitment checks and comply with our safeguarding and employment obligations, including the Department for Education's Keeping Children Safe in Education 2026.

Emergency contacts

We may collect:

- names and contact details
- relationship to the pupil or employee
- agreed authorisation or collection arrangements

We use this information to contact an appropriate person in an emergency and, where relevant, ensure pupils are released only to authorised individuals.

Referees



We may collect:

- your name and contact details
- your relationship to an applicant
- information you provide in a reference

We use this information to assess the suitability of applicants for employment, volunteering or governance roles.

Visitors

We may collect:

- name and contact details
- organisation
- vehicle details
- safeguarding or DBS information where required
- visitor-management records and CCTV footage

We use this information to manage access to the premises, safeguard pupils and maintain site security.

People who make complaints, requests or enquiries

We may collect:

- contact details
- nature of the complaint, request or enquiry
- related correspondence and the outcome

We use this information to respond, investigate where necessary, maintain appropriate records and comply with our legal obligations.

Website, network, Wi-Fi and school managed device users

We may collect information about the use of our networks, online services and school-managed devices. This may include IP addresses and device identifiers, account or username information, websites and online resources accessed, connection and security logs, attempted access to blocked content, search terms and filtering or monitoring alerts. Depending on the monitoring system used, an alert may also contain relevant content, such as text entered, images, messages or a screenshot of activity.

We use filtering systems to help prevent access to illegal, inappropriate or potentially harmful content. We may also use technical monitoring systems to identify activity that may indicate a safeguarding, online safety, cyber security or other serious concern. Monitoring alerts are reviewed by appropriately authorised staff and are not treated as proof that a concern has occurred.

Monitoring is normally limited to the school's networks and school-managed devices. Where a school-managed device continues to be filtered or monitored away from school, including at home, we will ensure that this is necessary, proportionate and clearly explained. We do not routinely monitor personal devices.

Access to monitoring information is restricted to authorised staff and relevant service providers who need it for safeguarding, system management, security or the investigation of a concern. Where necessary, relevant information may be added to the school's safeguarding, disciplinary, security or incident records.



Routine filtering and monitoring records are kept only for as long as necessary for the relevant safeguarding, security, monitoring or investigation purpose. Where information becomes part of another school record, the retention period applying to that record will apply.

For information about our use of Cookies, see our [Cookie Policy](#).

3. Use of CCTV

Where the school operates CCTV, images of pupils, staff, visitors and other individuals on school premises may be recorded. We use CCTV only where it is necessary and proportionate for purposes such as safeguarding, preventing and detecting crime, protecting school premises and property, managing site security, and investigating incidents or concerns.

Cameras are positioned to minimise unnecessary or excessive intrusion into individuals' privacy and, where appropriate, configured to block or obscure areas that do not need to be monitored. Cameras are not normally used in toilets, changing rooms or other areas where people would reasonably expect a high level of privacy. Audio recording and facial recognition are not used as part of the school's standard CCTV arrangements. Appropriate signage is displayed to make individuals aware that CCTV is in operation.

The school carries out and reviews a Data Protection Impact Assessment (DPIA) for its CCTV system to assess privacy risks and ensure that the use, location and operation of cameras remain justified and proportionate.

Access to footage is restricted to authorised individuals. Recordings are retained only for as long as necessary and may be shared with the police, insurers, legal advisers or other relevant organisations where this is necessary and lawful.

Further information can be found in our CCTV Policy which can be viewed [here](#).

4. Use of Artificial Intelligence (AI)

We may use approved Artificial Intelligence (AI) tools and AI-enabled features to support teaching, administration, communication and the effective running of the school. This may include approved AI-assisted transcription, meeting notes, summaries or action points within school-managed services. Where personal information is involved, we will only use AI where the proposed use has been assessed and appropriate data protection, security and human oversight arrangements are in place. We do not permit personal information to be entered into unapproved public or consumer AI tools. Further information about how this school currently permits staff to use AI is available in our Artificial Intelligence (AI) Privacy Notice Addendum which can be viewed [here](#).

5. Who we share personal information with

We only share personal information where this is necessary, lawful and proportionate.

Department for Education

We are required to provide certain pupil, workforce and governance information to the Department for Education (DfE) through statutory data collections, including the school census and school workforce census. The DfE may use and share this information for statutory functions, education policy, funding,



research and accountability purposes. You can find out more about how the DfE uses personal data provided by schools in its [Personal Information Charter](#) at www.gov.uk

Local authority

We may share personal information with our local authority where this is necessary to support admissions, education, attendance, safeguarding, SEND provision, school governance and other statutory functions. This may include sharing pupil and parent information to support school admissions, safeguarding and child protection responsibilities, and information needed to enable the local authority and the school to meet their respective legal duties. You can find out more about how the Local Authority uses personal data provided by schools in its Privacy Notice.

Health, social care and safeguarding

We may share personal information with health, social care and safeguarding professionals and other relevant bodies, including local authorities, the police, regulatory bodies and other organisations, where this is necessary to support an individual's health, care or welfare, or to fulfil safeguarding responsibilities.

This may include information about pupils, parents and carers, employees, other workers, volunteers, governors, trustees and others connected with the school. Where consent is required or appropriate, we will seek it before sharing personal information. However, we may share information without consent where this is necessary to comply with a legal obligation, perform a task in the public interest or exercise our official authority, fulfil our safeguarding responsibilities, protect someone from harm, manage a safeguarding concern or allegation, or enable another organisation to assess and manage a safeguarding risk, where doing so forms part of our own safeguarding responsibilities.

We ensure that any information shared is relevant, necessary and proportionate to the purpose and is shared securely.

Other schools and education settings

When a pupil transfers to another school or education setting, we will share the information needed to support the continuation of their education, safeguarding and welfare. This may include the pupil's Common Transfer File, educational records and relevant safeguarding information.

Where there are safeguarding concerns, we will ensure that relevant information is shared promptly and securely with the receiving school or setting in line with our legal obligations and safeguarding responsibilities. We will only share information that is necessary and proportionate for the purpose.

Examination boards, awarding organisations and moderators

We share relevant student information with examination boards, awarding organisations and moderators where this is necessary to enter students for qualifications, administer examinations and assessments, arrange access arrangements or reasonable adjustments, mark or moderate work, investigate examination matters and issue results and certificates.

We only share the information required for these purposes and in accordance with the relevant examination and awarding body requirements.

Youth support and careers services

We may share relevant information about students with the local authority, careers advisers and youth support services to support careers education, participation in education or training, and post-16 or post-18 transition and destination planning.



Ofsted

During an inspection, Ofsted may require access to school records containing personal information in order to assess the school's compliance with education, safeguarding and other regulatory requirements. Where this happens, access will be limited to information that is relevant to the inspection and handled in accordance with applicable legal and confidentiality requirements.

Police, courts and other public authorities

We may share personal information with the police, courts, local authorities or other public bodies where this is necessary and lawful. This may include complying with a legal obligation or court order, supporting a criminal or regulatory investigation, preventing or detecting crime, safeguarding an individual, or protecting someone from serious harm. We will only disclose information that is necessary and proportionate in the circumstances.

Research organisations

We may take part in local or national research projects that support education, safeguarding, public policy or the wellbeing of children and young people. Wherever possible, information will be anonymised or aggregated so that individuals cannot be identified.

Where identifiable personal information is required, we will only share it where there is an appropriate lawful basis, the research has been properly assessed, and suitable data protection and security safeguards are in place. Where appropriate, we will also provide relevant information to parents, carers or other affected individuals about how their data will be used and the rights they have.

Service providers

We use external providers to support the effective running of the school. These may include providers of:

- IT, technical support, cyber security, cloud, productivity and AI-enabled services
- management information, online learning, teaching, communication, filtering and monitoring systems
- payroll, finance, pensions, payments and other administrative services
- catering, transport, school trips, work experience, school transition, careers and other student support services
- professional, legal, HR, occupational health, training and other specialist advice
- school photography, music tuition, extracurricular activities and other services provided directly to pupils or families.

Where a provider processes personal data on our behalf, appropriate contractual, security and data protection arrangements are put in place to ensure personal information is protected and handled in accordance with data protection law.

Some providers may provide services directly to pupils or families and may act as separate data controllers in their own right. Our service providers may change from time to time. You can obtain details of the current providers we use by contacting us at admin@plymouthcast.org.uk.

6. Our lawful bases for processing



We process personal information where we have a lawful basis under the UK GDPR and the Data Protection Act 2018.

The main lawful bases we rely on are:

- **Public task** – where processing is necessary for us to provide education or perform our official functions
- **Legal obligation** – where we are required to process information by law
- **Contract** – where processing is necessary to enter into or perform a contract
- **Consent** – where you have a genuine choice and there is not another more appropriate lawful basis
- **Vital interests** – where processing is necessary to protect someone's life or safety
- **Legitimate interests** – where processing is necessary for our or another person's legitimate interests and these are not overridden by the individual's rights. We will not rely on this basis where the processing forms part of our public tasks or official functions.
- **Recognised legitimate interests** – where processing is necessary for a recognised legitimate interest specifically provided for in data protection legislation and this lawful basis is available to us. We will not rely on this basis where the processing forms part of our own public tasks or official functions.

Where we process Special Category Data, such as health, ethnicity, political opinions, religion, trade union membership or biometric data, we must also identify an additional condition for processing.

These may include:

- explicit consent
- employment, social security or social protection law
- vital interests
- substantial public interest, including safeguarding
- health or occupational health purposes
- legal claims
- information deliberately made public by the individual
- research, archiving or statistical purposes where applicable

Where we process information about criminal convictions or offences, we will ensure that a lawful basis and an appropriate condition under the Data Protection Act 2018 apply.

Further information about how we handle Special Category Data is available in our Appropriate Policy Document which is available to view [here](#).

7. How we keep your information secure

We use appropriate technical and organisational measures to protect personal information. These include:

- access controls based on roles and responsibilities
- multi-factor authentication where required
- encryption and secure systems
- secure storage for paper records
- appropriate visitor and premises security
- staff confidentiality and data protection training
- secure email and file-sharing arrangements
- due diligence and contracts with service providers
- regular backups and security updates



8. How long we keep your information

We keep personal information only for as long as it is needed for the purpose for which it was collected or to comply with legal, contractual, safeguarding, accounting or regulatory requirements. Once information is no longer required, it is securely deleted or destroyed. Further information is available in our Record Retention Schedule which is available to view [here](#).

9. International transfers

Some of our service providers may process personal information in countries outside the UK or EEA, even where the main service or Customer Data is stored within the UK or EEA.

Where we use cloud or AI-enabled services, we consider both where personal information is stored and whether any part of the service involves international processing or access from another country. Where personal information is transferred to a country outside the UK and the transfer is restricted under UK data protection law, we ensure that an appropriate transfer mechanism or safeguard is in place. This may include:

- UK adequacy regulations
- the UK International Data Transfer Agreement
- the UK Addendum to approved contractual clauses
- another lawful transfer mechanism

Where relevant, we also consider the contractual safeguards and international transfer arrangements provided by our service providers as part of our supplier due diligence.

Further information about international transfers relating to a particular service is available from the school on request.

10. Your data protection rights

You have the following rights in relation to your personal data:

- **Right to be informed** – know how and why we collect, use and share your personal data
- **Right of access** – request a copy of the personal data we hold about you
- **Right to rectification** – ask us to correct personal data that is inaccurate or incomplete
- **Right to erasure** – ask us to delete your personal data in certain circumstances
- **Right to restrict processing** – ask us to limit how we use your personal data in certain circumstances
- **Right to object** – to object to certain uses of your personal data, including direct marketing and, in some circumstances, processing carried out in the public interest
- **Right to data portability** – ask us to provide your personal data to you, or transfer it to another organisation, where this right applies
- **Rights relating to automated decision-making** – where significant decisions are made solely by automated means, to have appropriate safeguards in place, including the right to human intervention and to challenge the decision
- **Right to complain** – to complain to the school if you are unhappy with how your personal data or data protection rights have been handled. If you remain dissatisfied, you can complain to the Information Commissioner's Office (ICO) at www.ico.org.uk and escalate this through the courts.



Students may exercise their own data protection rights where they have sufficient understanding to do so. Students aged 16 and over will normally be expected to exercise their rights themselves. For students under 16, we will consider their age, maturity and understanding when deciding whether they can exercise their rights independently. A parent or carer may act on a student's behalf where the student has authorised them to do so, or where the school considers this appropriate having regard to the student's age, understanding and best interests.

11. Complaints and contact details

Data protection complaints

If you are unhappy with how we have handled your personal information or your data protection rights, you can make a data protection complaint to Plymouth CAST:

- Edmund Rice Building, 21 Boniface Lane, Manadon Park, Plymouth, PL5 3AG;
- Email: admin@plymouthcast.org.uk;
- Tel: 01752 686710.

We will acknowledge a data protection complaint within 30 days, take appropriate steps to investigate it, keep you informed where appropriate and provide the outcome without undue delay. If you remain dissatisfied, you may complain to the Information Commissioner's Office and escalate this through the courts.

Data Protection Officer

Our Data Protection Officer is:

Firebird Data Protection Consultancy Limited

Email: DPO@firebirdltd.co.uk

Our outsourced Data Protection Officer oversees our data protection compliance and provides independent advice to the school.

Changes to this notice

We may update this privacy notice from time to time to reflect changes in our processing activities, law or regulatory guidance. The latest version will be available on our website.

Last updated: September 2026