Privacy Notice – Primary 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.

This Privacy Notice is for our Plymouth CAST Primary Schools.

Our registered address is Edmund Rice Building, 21 Boniface Lane, Manadon Park, Plymouth, PL5 3AG. As the data controller, we are responsible for protecting the personal information we hold about you. Our Data Protection Registration Number is ZA022556.

We respect your privacy and take our legal responsibilities seriously. This notice explains:

1. How we collect personal information
2. What personal data we collect and why
3. Who we share information with
4. Our legal basis for processing
5. How we keep your data secure
6. How long we retain your data
7. Oversees data transfers
8. Your data protection rights
9. Contact us

1. How we collect personal information

We collect personal data directly when you:

- Register your child with us
- Apply for a job, volunteer or governor role
- Visit our premises or website
- Make an enquiry, request or complaint

We also receive personal data indirectly, for example from:

- Previous schools when a pupil transfers
- External professionals (e.g. health or social care)
- Parents/employees providing emergency contacts
- Public authorities (eg local authority, police, courts)
- Referees for job applicants, volunteers and governors

©2025 Firebird Data Protection Consultancy Limited

2. What personal data we collect and why

We collect and use personal information about the people who interact with us. This helps us run our school effectively and ensure we meet our legal obligations. The following is a summary of the type of personal data we hold about key groups of people and how we use it:

Pupils

We collect and process the following information about pupils to support their education, safety, and wellbeing, and to meet our statutory obligations:

- **Identifiers and contact details** – name, date of birth, home address, unique pupil number.
- **Characteristics** – gender, ethnicity, nationality, English as an Additional Language (EAL), Special Educational Needs and Disabilities (SEND) status, eligibility for free school meals and Looked-After Child (LAC) status.
- **Faith and beliefs** – religion or belief (including "no religion" or none declared). For admissions to faith schools, this may include baptism certificates, evidence of religious practice (e.g. attendance), clergy or minister references, or other information required by the school's admissions policy
- **Education** – attainment, progress, assessments, reports and transition records.
- **Attendance** – registers, reasons for absence, and punctuality records.
- **Health and dietary** – medical conditions, disabilities, allergies, accidents and first aid records.
- **Behaviour and welfare** – behaviour logs, rewards, sanctions, exclusions, pastoral records, and relevant family circumstances (including domestic abuse).
- **Safeguarding** – concerns, referrals, interventions and protection measures.
- **Special educational needs** – Education Health and Care Plans (EHCPs), Individualised Education Plans (IEPs) and records of specialist involvement.
- **Images** – photographs and videos of classroom activities, trips, performances, and official school photographs (e.g. individual, class, year group, leavers), as well as CCTV footage.
- **Consents** – permissions for trips, internet use, image use, and medical treatment.

We use this information to identify pupils, keep them safe, and support their learning and wellbeing. It also enables us to provide high-quality teaching and care, meet statutory data collection requirements, monitor equality, manage admissions fairly, and work in partnership with families to support each child's development and pastoral care.

CCTV images are processed for the purposes of crime prevention and detection, safeguarding, and the safety of individuals on site. They may also be used as evidence in relation to incidents, investigations, or complaints. Other images may be used for identification, school administration, celebrating school life, and promotional purposes, where appropriate consents have been obtained.

©2025 Firebird Data Protection Consultancy Limited

Parents and carers

We collect and process the following information about parents and carers in order to support the education, safety, and wellbeing of pupils, and to meet our statutory and operational obligations:

- **Identifiers and contact details** – Name, home address, telephone number, email address, and work contact details.
- **Family circumstances** – parental responsibility, guardianship, court orders, separation/divorce details, domestic abuse, and any other information relevant to the pupil's welfare and safeguarding.
- **Faith and beliefs** – religion or beliefs (including "no religion" or none declared). For admissions to faith schools, this may include baptism or marriage certificates, details of religious practice (e.g. church, mosque, synagogue attendance), clergy or minister references, or other information required by the school's admissions policy.
- **Financial** – payment details for school meals, trips, activities, and souvenirs (e.g. Year 6 or Year 11 leavers' gifts), as well as free school meal eligibility status.
- **Armed forces** – whether the parent/carer is a serving member of the armed forces
- **Images** – CCTV footage, visitor management system entries.

We use this information to communicate effectively with parents and carers, support pupil learning, promote wellbeing, and act in each child's best interests. It helps us to understand family circumstances, manage admissions fairly, and respect faith or beliefs. We also process this information to administer payments, determine eligibility for financial support, record consents, fulfil statutory reporting requirements, and maintain site safety and security. CCTV images are processed for the purposes of crime prevention and detection, safeguarding, and the safety of individuals on site. They may also be used as evidence in relation to incidents, investigations, or complaints.

Employees

We collect and process the following information about employees to manage employment relationships fairly, safely, and lawfully, and to meet our statutory and contractual obligations:

- **Identifiers and contact details** – Name, date of birth, employee or teacher number, National Insurance Number, biometric identifiers, car registration number, home address, telephone number, email address and emergency contact details.
- **Characteristics** – gender, age and ethnicity.
- **Recruitment** – job application records, qualifications, training, right to work documentation, references, Disclosure and Barring Service (DBS) and Barred List results (where required).
- **Employment records** – start date, role, contract, salary, working hours, appraisal and performance, professional development, disciplinary and grievance records.
- **Payroll and pensions** – bank account details, salary, tax, pension contributions, payroll records.

©2025 Firebird Data Protection Consultancy Limited

- **Health and dietary** – medical conditions, disabilities, occupational health assessments, dietary needs and accident/first aid records.
- **Absence** – records of sickness, maternity/paternity, parental and adoption leave records, compassionate leave, fit notes and return-to-work forms.
- **Faith and beliefs** – religious affiliation, observance of religious festivals or prayer times, dietary requirements linked to faith, expressions of philosophical or other beliefs. For faith-based schools, this may include information gathered during recruitment or for assessing role suitability (practicing faith, reference from clergy).
- **Trade union membership** – membership details, branch and involvement in union activities.
- **Images** – staff ID photographs, CCTV footage, visitor management system entries, photographs or videos taken at events, for training or for promotional purposes.
- **Consent** – preferences relating to optional uses of personal data (e.g. wellbeing surveys, promotional photography).

We use this information to recruit, train, and appraise staff, administer payroll and pensions, and comply with tax and reporting obligations. Employee records support the monitoring of equality and diversity, delivery of safeguarding and safer recruitment duties, and provision of reasonable adjustments to support health, wellbeing and faith needs.

Employment records, absence data, and emergency contacts enable us to plan workforce capacity, manage attendance, and respond effectively in emergencies. We also process trade union membership information where relevant to statutory rights or collective bargaining.

CCTV images are processed for crime prevention and detection, safeguarding and the safety of individuals on site. They may also be used as evidence in relation to incidents, investigations, or complaints. Other images may be used for security and identification, administration, celebrating school life, or promotional purposes where consent has been provided.

Temporary workers, contractors, trainee/student teachers

We collect and process the following information to manage temporary and agency staff, contractors, and trainee or student teachers fairly, safely, and lawfully, and to meet our statutory and contractual obligations:

- **Identifiers and contact details** – name, teacher number, home address, telephone number, email address and biometric identifiers.
- **Characteristics -** gender, age and ethnicity.
- **Recruitment** – qualifications, training, right-to-work documentation, references, and Disclosure and Barring Service (DBS) and Barred List results (where required).
- **Contract information** – start date, role, hours of work, bank/payment details, and pension/tax details.
- **Health and dietary** – medical conditions, disabilities, dietary needs, and accident/first aid records.

©2025 Firebird Data Protection Consultancy Limited

- **Faith and beliefs** – religious affiliation, observance of religious festivals or prayer times, dietary requirements linked to faith, and expressions of philosophical or other beliefs. For faith-based schools, this may include information gathered during recruitment or for assessing role suitability (e.g. practising faith, references from clergy).
- **Images** – ID photographs, CCTV footage, visitor management system entries, and photographs or videos taken at events, for training, or for promotional purposes.
- **Consent** – preferences relating to optional uses of personal data (e.g. use of images for promotional materials).

We use this information to recruit appropriately, confirm suitability to work with children, administer contracts, make salary or fee payments, and meet tax, pension, and reporting obligations. We also use it to monitor equality and diversity, fulfil safeguarding and safer recruitment requirements, and make reasonable adjustments to support health, wellbeing, and faith needs. Contract and attendance information supports effective workforce planning, while emergency contact details ensure we can respond quickly in urgent situations.

CCTV images are processed for crime prevention and detection, safeguarding, and the safety of individuals on site. They may also be used as evidence in relation to incidents, investigations, or complaints. Other images may be used for identification and security, administration, celebrating school life, or promotional purposes where appropriate consent has been provided.

Governors

We collect and process the following information about governors in order to manage governance effectively, transparently, and in line with statutory requirements:

- **Identifiers and contact details** – name, date of birth, home and former addresses, telephone number, and email address.
- **Governance role information** – appointment and term of office, governor type, appointing body, committee memberships, positions of responsibility, and meeting attendance records.
- **Characteristics** – gender, age, ethnicity.
- **Declarations and checks** – eligibility confirmations, declarations of interests, Disclosure and Barring Service (DBS) and Section 128 checks, and disqualification criteria.
- **Health and dietary information** – health conditions, disabilities, and dietary needs.
- **Faith and beliefs** – religious affiliation, observance of religious festivals or prayer times, dietary requirements linked to faith, and expressions of philosophical or other beliefs. For faith-based schools, this may include information gathered at appointment or for role suitability (e.g. practising faith, references from clergy).
- **Images** – ID photographs, CCTV footage, visitor management system entries, and photographs or videos taken at events, for training, or for promotional purposes.

We use this information to maintain accurate governance records, allocate responsibilities, monitor attendance, and meet statutory reporting requirements. Declarations and safeguarding checks confirm eligibility, suitability, and freedom from conflicts of interest.

©2025 Firebird Data Protection Consultancy Limited

Equality and religious belief data enable us to meet diversity duties and, in the case of faith schools, confirm that governors meet specific role requirements. Health and dietary information is used to support wellbeing and to make reasonable adjustments where necessary.

CCTV images are processed for crime prevention and detection, safeguarding, and the safety of individuals on site. They may also be used as evidence in relation to incidents, investigations, or complaints. Other images may be used for security and identification, administration, celebrating school life, or promotional purposes where appropriate consent has been provided.

Volunteers

We collect and process the following information about volunteers in order to manage volunteering arrangements safely, fairly, and in line with our safeguarding responsibilities:

- **Identifiers and contact details** – name, address, telephone number, and email address.
- **Disclosure and Barring Service (DBS) checks** – DBS certificate number and outcome, and Barred List checks where required.
- **Training and qualifications** – relevant training records and certificates.
- **Volunteering records** – dates, activities, events, or trips attended.
- **Health and dietary information** – health conditions, disability information, and dietary needs.
- **Images** – ID photographs, CCTV footage, visitor management system entries, and photographs or videos taken at events, training, or for promotional purposes.
- **Consent** – preferences relating to optional uses of personal data (e.g. use of images for promotional purposes).

We use this information to confirm suitability to volunteer, maintain accurate records, and ensure that safeguarding standards are upheld. Health and dietary details enable us to support wellbeing and make reasonable adjustments where needed. Volunteering records help us to manage attendance, involvement in activities, and deployment across school events.

CCTV images are processed for crime prevention and detection, safeguarding, and the safety of individuals on site. They may also be used as evidence in relation to incidents, investigations, or complaints. Other images may be used for identification and security, administration, celebrating school life, or promotional purposes where appropriate consent has been provided.

Job applicants

We collect and process the following information about job applicants in order to manage recruitment fairly, transparently, and in line with statutory safeguarding obligations:

- **Identifiers and contact details** – name (including former names), date of birth, home and previous addresses, telephone number, email address, and National Insurance number.
- **Application details** – position applied for, personal statement, employment history (including reasons for leaving previous or current roles), and referee details. Shortlisted

©2025 Firebird Data Protection Consultancy Limited

applicants are also required to provide self-declarations relating to criminal records, prohibition from teaching, involvement with the police or social care, disqualifications, and relevant overseas information.

- **Education and experience** – qualifications, academic achievements, training, professional development, and employment history relevant to skills, knowledge, and experience.

We use this information to communicate with applicants, assess their suitability for the role, and evaluate their skills, knowledge, and experience. This ensures that appointments are made on merit, in line with safer recruitment principles, and in compliance with our legal and safeguarding obligations under the Department for Education's Keeping Children Safe in Education (KCSIE) 2025.

As required by KCSIE 2025, we also carry out a range of pre-employment checks before any appointment is confirmed. These include verification of identity, right to work in the UK, qualifications, references, and criminal record checks (including enhanced DBS and Barred List checks where applicable).

In addition, for shortlisted candidates we conduct proportionate online searches of publicly available information. These searches are undertaken after shortlisting and before interview and are carried out solely to help identify any issues that may be relevant to an applicant's suitability to work with children and young people.

Emergency contacts (for pupils and employees)

We collect and process the following information about emergency contacts in order to act quickly and safely in urgent situations, and to support the welfare of pupils and employees:

- **Identifiers and contact details** – name, address, telephone number, and email address.
- **Relationship** – the individual's relationship to the pupil or employee (e.g. grandparent, neighbour, partner).
- **Authorisation details** – passwords or agreed pupil collection arrangements.
- **Images** – CCTV footage, visitor management system entries, and photographs or videos taken at events, training, or for promotional purposes.

We use this information to ensure that, in the event of an emergency, we can contact the right person without delay. For pupils, it also allows us to confirm that children are released only to authorised individuals. Authorisation details, such as passwords or agreed collection arrangements, help us to maintain pupil safety at the end of the school day and during emergencies.

CCTV images are processed for crime prevention and detection, safeguarding, and the safety of individuals on site. They may also be used as evidence in relation to incidents, investigations, or complaints. Other images may be used for identification and security, administration, celebrating school life, or promotional purposes where appropriate consent has been provided.

©2025 Firebird Data Protection Consultancy Limited

Referees (for job applicants, volunteers, governors)

We collect and process the following information about referees in order to support recruitment, volunteering, and governance appointments, and to meet our safer recruitment and safeguarding responsibilities:

- **Identifiers and contact details** – name, address, telephone number, and email address.
- **Relationship** – the referee's relationship to the applicant (e.g. previous employer, colleague, mentor).
- **Reference** – the information you provide about the applicant's suitability, character, skills, and experience.

We use this information to verify the background and suitability of individuals applying to work, volunteer, or serve as governors within the school. Contact details and the stated relationship to the applicant allow us to confirm the context of the reference, while the content of the reference provides an informed assessment of the applicant's character, competence, and overall suitability for the role.

This process forms an essential part of our safer recruitment practices and helps us to discharge our statutory safeguarding duties in line with the Department for Education's Keeping Children Safe in Education (KCSIE) 2025.

Visitors

We collect and process the following information about visitors to our premises in order to maintain safety, security, and safeguarding standards:

- **Identifiers and contact details** – name and telephone number.
- **Organisation details** – the name of the company or organisation represented.
- **Vehicle details** – car registration number, if parked on school premises.
- **Disclosure and Barring Service (DBS)** – certificate number or confirmation that DBS checks have been undertaken by their employer), where required for safeguarding.
- **Images** – CCTV footage and entries on the visitor management system.

We use this information to identify and record who is on our premises at any given time, support safeguarding requirements, and maintain site security. Organisation details provide additional context where visitors are attending on behalf of external agencies or service providers. Vehicle details support safe and effective management of on-site parking.

CCTV images are processed for crime prevention and detection, safeguarding, and the safety of individuals on site. They may also be used as evidence in relation to incidents, investigations, or complaints. Other images may be used for identification and security, administration, celebrating school life, or promotional purposes where appropriate consent has been provided.

©2025 Firebird Data Protection Consultancy Limited

People who make a complaint, request or enquiry

We collect and process the following information from individuals who contact us with a complaint, request, or enquiry:

- **Identifiers and contact details** – name, address, telephone number, and email address.
- **Case details** – description of the complaint, request, or enquiry, records of correspondence, and the case outcome.

We use this information to identify you, respond to your enquiry or complaint, and maintain accurate records of the outcome. Keeping case details and correspondence allows us to manage follow-up enquiries, appeals, or tribunal proceedings where necessary.

This processing also ensures we can meet our legal and administrative responsibilities, demonstrate accountability in decision-making, and provide a fair and transparent process when handling complaints or requests.

Website users

When you visit our website, we collect standard internet log information and details about how the site is used. This may include data such as pages visited, length of time on pages, and navigation paths. Collecting this information helps us to understand how our website is being used, identify which pages are most frequently visited, and improve both the content and usability of the site.

This information is processed in an anonymised and aggregated form so that it does not identify individual visitors. We do not attempt to discover the identities of those who visit our website, and we do not link the information collected with any personally identifiable data from other sources.

For further details about the cookies we use and how you can manage them, please see our Cookie Policy.

3. Who we share information with

We only share information where it is necessary, lawful and proportionate. Examples include:

Department for Education (DfE):

We have a legal duty to share certain information about pupils, employees and governors with the Department for Education (DfE), so it can carry out its statutory responsibilities.

- **Pupils -** We submit data through the '*school census'* under Regulation 5 of *The Education (Information About Individual Pupils) (England) Regulations 2013*. This data is held in the *National Pupil Database (NPD)* and may be shared with approved third parties for research and education purposes.
- **Employees** – We submit data through the '*workforce census'* under Section 5 of *The Education (Supply of Information about the School Workforce) (England) Regulations 2007* (as amended). The DfE may share this data with third parties who promote children's education and well-being or support the effective use of school staff.

©2025 Firebird Data Protection Consultancy Limited

- **Governors** – Under Section 538 of the *Education Act 1996*, we must share details of governors and governance arrangements with the Secretary of State, which are published on the DfE's *Get Information About Schools (GIAS)* register.

Find out more:

- School census and data collections
- National Pupil Database privacy notice
- Workforce census information
- DfE Personal Information Charter
- Get Information About Schools (GIAS) register

Local Authority:

We are legally required to share certain information with our local authority so that both organisations can discharge their statutory duties effectively:

- **Pupils and parents** – information may be shared to support admissions under the School Admissions Code We are also required to share safeguarding information under *Section 11 of the Children Act 2004* (duty to safeguard and promote welfare) and *Section 47 of the Children Act 1989* (duty to investigate and take action to protect children).
- **Employees** – workforce information must be shared under Regulation 5 of the *Education (Supply of Information about the School Workforce) (England) Regulations 2007* (as amended).
- **Governors** – appointment and resignation details must be shared with the local authority for statutory school governance purposes.
- **Concerns or allegations –** under the Department for Education's *Keeping Children Safe in Education 2025,* the school is required to share information about anyone working in the school who provides education to pupils under the age of 18, where there are concerns or allegations of harm. This includes teachers, supply teachers, volunteers and contractors.

Health professionals:

We may share pupil information with relevant health professionals (such as educational psychologists, school nurses, or health visitors) to support pupils' education, wellbeing, and pastoral care. Wherever possible, this will be done with parental consent. However, information may also be shared without consent where necessary to fulfil our statutory duties or to safeguard a child.

Other schools:

When a pupil transfers to another school, we are required to share their Common Transfer File and educational record under the Education (Pupil Information) (England) Regulations 2005. Where we have concerns about a pupil's safety, we are also legally obliged to share relevant safeguarding information with the receiving school, in line with the Department for Education's Keeping Children Safe in Education (KCSIE) 2025. This ensures continuity of safeguarding and

©2025 Firebird Data Protection Consultancy Limited

welfare support for the child. Further information about our safeguarding practices can be found on our website.

Standards and Testing Agency:

We are legally required to share information about pupils in Year 2 and Year 6 with the Standards and Testing Agency (STA). This enables the Agency to administer and report on Key Stage 1 and Key Stage 2 national curriculum assessments (SATs). Further information about SATs, including how the data is used, can be found on the government's website.

Ofsted:

During inspections, we may be required to provide Ofsted inspectors with access to a sample of the school's records. These records may contain identifiable personal information. Inspectors will only view this information for the purposes of the inspection. Any personal data seen by inspectors will not be taken away, retained, or used in their reports.

Law enforcement and courts:

We may be required to share personal information with the police, other law enforcement agencies, or the courts. Such disclosures may be necessary in order to assist with investigations, comply with a court order, prevent or detect crime, or protect and safeguard individuals who may be at risk.

Research:

From time to time, we may be asked to contribute to local or national research projects that involve the use of pupil data and are endorsed by the Department for Education (DfE). These projects are designed to improve understanding of education, outcomes, and the wellbeing of children and young people.

If identifiable personal data is required for a research project, we will inform parents and carers in advance and provide the opportunity to opt out of their child's data being included. Where possible, data will be anonymised or aggregated so that individuals cannot be identified.

Service providers:

We use a range of external companies and organisations to support the effective running of the school. These include providers of IT support, online learning and communication platforms, payroll and finance services, professional advisers, training providers, catering, transport, and transition services.

These organisations act as our 'data processors'. Where personal information needs to be shared or stored using their systems, this is done under contract and in compliance with the UK GDPR, ensuring that personal data is protected and individuals' rights are upheld.

We also work with providers who deliver services directly to pupils or parents, such as school photographers, music tutors, extra-curricular clubs, or school trip organisers. Where consent is required, we will seek this in advance unless it is reasonable to expect us to act on your behalf (for example, booking a place on a trip).

©2025 Firebird Data Protection Consultancy Limited

Our service providers may change from time to time. For details of the current companies or individuals we work with, please contact us at admin@plymouthcast.org.uk.

4. Our legal basis for processing

We process personal information when we have a lawful basis to do so under the UK GDPR and Data Protection Act 2018. The main legal bases we rely on are:

- **Public task (official duties/public interest):** the primary basis for processing pupil data and other information necessary to deliver education and carry out statutory functions.
- **Legal obligation:** where processing is required by law (e.g. sharing information with the Department for Education, HMRC, the courts, or the local authority).
- **Contract:** where processing is necessary to meet contractual obligations (e.g. for employees, agency staff, parents using paid services, or agreements with service providers).
- **Consent:** In limited circumstances where we cannot rely on another lawful basis, we will rely on consent (eg processing biometric data, using photographs or videos for publicity, marketing or fundraising communications, or providing access to optional third-party services.
- **Vital interests:** where processing is necessary to protect life or prevent serious harm (e.g. in medical emergencies or safeguarding situations).
- **Legitimate interests:** where there is a clear benefit to the school or individuals, the impact on privacy is minimal, and data subjects have a reasonable expectation that their data will be processed in this way.

When processing special category data (such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health information, or data relating to sex life or orientation), we must also rely on an additional lawful basis. The main ones we use are:

- **Explicit consent** – eg when collecting fingerprints or facial recognition data.
- **Employment, social security or social protection law** – eg safeguarding, health and safety, equality monitoring and tax compliance.
- **Vital interests** – eg sharing health details with emergency services when someone's life is at risk and they are unable to consent.
- **Not-for-profit bodies** – eg processing personal data by religious, charitable or trade union organisations about their members.
- **Legal claims** – eg establishing, exercising or defending legal claims.
- **Substantial public interest** – eg safeguarding children or assisting law enforcement.
- **Assessment of working capacity** – eg occupational health reviews to determine whether an employee is fit to return to work after illness or injury.

©2025 Firebird Data Protection Consultancy Limited

This list is not exhaustive. For further details about how we handle special category data and criminal offence data, please see our Appropriate Policy Document which is available to view on our website.

5. How we keep your data secure

We take the security of personal data very seriously and use a range of technical and organisational measures to protect it from loss, misuse, unauthorised access, disclosure, alteration, or destruction. These measures include:

- **Access controls** – only authorised staff can access personal data, with permissions based on role and responsibility.
- **Secure systems** – encrypted servers for digital records, and secure locked storage for paper files.
- **Site and visitor security** – robust visitor management procedures, CCTV monitoring, and controlled site access.
- **Staff responsibilities** – all staff, volunteers, and governors are subject to appropriate DBS checks, confidentiality obligations, and mandatory training on data protection and information security, supported by clear school policies.
- **Secure communications** – encrypted email and secure file-sharing platforms for external transfers of information.
- **Service providers** – due diligence on third-party suppliers, data processing contracts, and the use of secure systems for handling data.
- **Risk management** – Data Protection Impact Assessments (DPIAs) where required, to identify and mitigate risks before new systems or processes are introduced.
- **System resilience** – regular data backups, timely security updates, and anti-virus/malware protection across our IT systems.

These safeguards are designed to ensure that personal data is handled safely, securely, and in compliance with the UK GDPR and Data Protection Act 2018.

6. How long we retain your data

We only keep personal information for as long as it is needed to fulfil operational purposes or to meet our legal, contractual, accounting, reporting, or archiving obligations. Once the relevant retention period has expired, data is securely deleted, shredded, or otherwise destroyed in a safe and confidential manner.

For full details of how long different categories of information are retained, please see our Record Retention Schedule which is available to view on our website.

7. Overseas data transfers

©2025 Firebird Data Protection Consultancy Limited

Most of our data is stored in the UK or the European Economic Area (EEA), however some of our service providers may process personal data outside these areas. Where this occurs, we ensure that appropriate safeguards are in place, such as the use of UK International Data Transfer Agreements or other recognised lawful transfer mechanisms. These safeguards ensure that your personal information is protected and handled securely in accordance with UK data protection laws.

8. Your data protection rights

Under the UK GDPR and the Data Protection Act 2018**,** you have the following rights in relation to your personal data:

- **Right to be informed** – to know how your personal data is collected, used and shared.
- **Right of access** – to request a copy of the personal data we hold about you.
- **Right to rectification** – to ask us to correct data that is inaccurate or incomplete.
- **Right to erasure** – to request deletion of your personal data in certain circumstances.
- **Right to restrict processing** – to limit how we use your personal data in certain circumstances.
- **Right to object** – to object to your data being processed for public interest tasks or direct marketing.
- **Right to data portability** – to request that your data is transferred to another organisation or provided to you, where applicable.
- **Rights related to automated decision-making** – to prevent decisions being made about you solely by automated means (including profiling).
- **Right to complain** – to raise a concern with the school if you are unhappy with how your data has been handled. If the issue remains unresolved, you have the right to escalate your complaint to the Information Commissioner's Office (ICO) at www.ico.org.uk

9. Contact us

Exercising your rights

If you have any queries regarding this privacy notice, or want to exercise any of your data protection rights, contact us at:

Edmund Rice Building, 21 Boniface Lane, Manadon Park, Plymouth, PL5 3AG;

Email: admin@plymouthcast.org.uk;

Tel: 01752 686710.

You will not usually need to pay a fee, and we will respond within one calendar month. For more details about your data protection rights, visit www.ico.gov.uk

Complaints

©2025 Firebird Data Protection Consultancy Limited

If you are unhappy with how your information has been managed and want to make a complaint, please follow our Complaints Procedure which is available to view on our website. If you remain dissatisfied with the outcome of your complaint, you can refer the matter to the Information Commission at www.ico.org.uk

Data Protection Officer

Our school's Data Protection Officer is Firebird Data Protection Consultancy Limited, who oversee our data protection compliance. You can contact them directly at DPO@firebirdltd.co.uk.

Changes to this notice

We may update this notice from time to time. The latest version will always be available on our website. Last updated: September 2025.

©2025 Firebird Data Protection Consultancy Limited