Plymouth CAST

Data Protection Policy

2022-2023

Version: 2.1

Policy Date: July 2022

Approved by: CAST Board

Next review date: July 2023

Contents

1 Introduction and purpose 3

2 Scope 3

3 Definitions 3

4 Roles and responsibilities 4

4.1 Board of Trustees 4

4.2 Headteacher / Executive Head of School] 4

4.3 Data Protection Officer 4

4.4 Employees, temporary staff, contractors, visitors 5

5 Policy content 5

5.1 Data Protection Principles 5

5.2 Lawfulness, fairness and transparency 5

5.3 Purpose limitation 8

5.4 Data minimisation 8

5.5 Accuracy of data 8

5.6 Storage limitation and disposal of data 8

5.7 Security of personal data 8

5.8 Technical security measures 8

5.9 Organisational security measures 9

5.10 Rights of Data subjects 10

5.11 Handling requests 10

5.12 Data protection by design and default 10

5.13 Joint controller agreements 10

5.14 Data processors 10

5.15 Record of processing activities 11

5.16 Management of personal data security breaches 11

5.17 Data Protection Impact Assessments 12

5.18 Data sharing 13

5.19 Appointment of a Data Protection Officer 13

6 Policy history 14

Appendix 1 15

1 Introduction and purpose

1.1 This policy sets out Plymouth CAST commitment to handling personal data in line with the General Data Protection Regulation 2016 (UK GDPR) and the Data Protection Act 2018 (collectively referred to as the data protection legislation).

1.2 The Trust is the data controller for the personal data it processes and is registered with the Information Commissioner's Office (ICO) under registration number ZA022556. Details about this registration can be found at www.ico.org.uk

1.3 The purpose of this policy is to explain how the Trust handles personal data under the data protection legislation, and to inform employees and other individuals who process personal data on the Trust's behalf of the Trust's expectations in this regard.

2 Scope

2.1 This policy applies to the processing of personal data held by the Trust. This includes personal data held about pupils, parents/carers, employees, temporary staff, governors, visitors, and any other identifiable data subjects.

2.2 This policy should be read alongside the Personal Data Breach Handling Procedure and Data Protection Request Handling Procedure.

3 Definitions

3.1 There are several terms used in the data protection legislation and in this policy, which must be understood by those who process personal data held by the Trust. These are:

- Personal data
- Special categories of personal data
- Processing
- Data subject
- Data controller
- Data processor

3.2 These terms are explained in Appendix 1.

4 Roles and responsibilities

4.1 Board of Trustees

4.1.1 The Board of Trustees has overall responsibility for ensuring the Trust implements this policy and continues to demonstrate compliance with the data protection legislation.

4.1.2 This policy shall be reviewed by the Board of Trustees on an annual basis.

4.2 Headteacher/Executive Head

4.2.1 The Headteacher has day-to-day responsibility for ensuring this policy is adopted and adhered to by employees and other individuals processing personal data on the Trust's behalf.

4.3 Data Protection Officer

4.3.1 The Data Protection Officer (DPO) is responsible for carrying out the tasks set out in Article 39 of the General Data Protection Regulation (the UK GDPR). In summary, the DPO is responsible for:

- informing and advising the Trust of their obligations under the data protection legislation
- monitoring compliance with data protection policies
- raising awareness and providing training material to employees
- carrying out audits on the Trust's processing activities
- providing advice regarding Data Protection Impact Assessments and monitoring performance
- co-operating with the Information Commissioner's Office
- acting as the contact point for data subjects exercising their rights

4.3.2 The DPO shall report directly to the governing body and Senior Leadership Team and shall provide regular updates on the Trust's progress and compliance with the data protection legislation.

4.3.3 The Trust's DPO is an external consultant who performs the role under a service contract. The DPO is Amber Badley (Firebird Data Protection Consultancy Limited), who can be contacted through the Trust at Admin@plymouthcast.org.uk or directly via DPO@firebirdltd.co.uk

4.3.4 The DPO is supported in their role by a Trust employee, this person is known as the DPO's Data Protection Link Officer. All enquiries, complaints, requests, and suspected breaches of security should be referred to the Data Protection Link Officer in the first instance, who will then notify the DPO.

4.4 Employees, temporary staff, contractors, visitors

4.4.1 All employees, temporary staff, contractors, visitors, and other individuals processing personal data on behalf of the Trust, are responsible for complying with the contents of this policy.

4.4.2 All individuals shall remain subject to the common law duty of confidentiality when their employment or relationship with the Trust ends. This does not affect an individual's rights in relation to whistleblowing.

4.4.3 Failure to comply with this policy may result in disciplinary action or termination of employment or service contract.

4.4.4 All individuals who handle the Trust's data shall be made aware that unauthorised access, use, sharing or procuring of data, may constitute a criminal offence under the Data Protection Act 2018 and/or the Computer Misuse Act 1990.

5 Policy content

5.1 Data Protection Principles

5.1.1 The GDPR provides a set of principles which govern how the Trust handles personal data. In summary, these principles state that personal data must be:

- processed lawfully, fairly and in a transparent manner
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant, and limited to what is necessary for the purpose it was processed
- accurate and where necessary kept up to date
- kept for no longer than is necessary
- processed in a manner that ensures appropriate security of the data

5.1.2 The Trust shall have appropriate measures and records in place to demonstrate compliance with the data protection principles (accountability principle).

5.1.3 All individuals processing personal data controlled by the Trust shall comply with the data protection principles in the following manner:

5.2 Lawfulness, fairness, and transparency

5.2.1 Lawful processing

5.2.2 Personal data will only be processed where there is a lawful basis for doing so. This will be where at least one of the following applies:

- The data subject has given consent.
- It is necessary for contractual purposes.
- It is necessary to comply with the law.
- It is necessary to protect someone's life.
- It is necessary to carry out our official tasks or functions, or other specific tasks in the public interest.
- It is necessary our legitimate interests as a Trust or third party, except where such interests are overridden by the data subject.

5.2.3 When special categories of personal data are processed (i.e. data which reveals a person's racial or ethnic data; political opinions; religious or philosophical beliefs; trade union membership; genetic or biometric data; health data; sex life or sexual orientation), this shall only be done where a lawful basis has been identified from the list above, and one from the following list:

- The data subject has given explicit consent.

- The processing is necessary for employment, social security, or social protection (e.g. safeguarding individuals at risk; protection against unlawful acts; prevention against fraud).
- It is necessary to protect the data subject's life and they are physically or legally incapable of giving consent.
- The data has been made public by the data subject.
- The processing is necessary in relation to legal claims.
- The processing is necessary for reasons of substantial public interest.
- The processing is necessary for health or social care.
- The processing is necessary for public health.
- The processing is necessary for archiving, research, or statistical purposes.

5.2.4 Consent

5.2.5 Most of the Trust's processing of personal data will not require consent from data subjects (or their parents/carers as appropriate), as the Trust needs to process this data in order to carry out its official tasks and public duties as a Trust.

5.2.6 However, there are circumstances when the Trust is required to obtain consent to process personal data, for example:

- To collect and use biometric information (e.g. fingerprints and facial images) for identification purposes.
- To send direct marketing or fundraising information by email or text, where the data subject would not have a reasonable expectation that their data would be used in this way or have objected to this.
- To take and use photographs, digital or video images and displaying, publishing or sharing these in a public arena (such as on social media, on the Trust/school website; in the Press; in the prospectus; newsletter etc), where the data subject would not have a reasonable expectation that their images would be used in this way, or the rights of the data subject override the legitimate interests of the Trust.
- To share personal data with third parties (e.g. professionals, agencies, or organisations) where the data subject has a genuine choice as to whether their data will be shared, for example when offering services which the data subject does not have to accept or agree to receive.

5.2.7 When the Trust relies on consent as its lawful basis, it shall ensure the person providing it has positively opted-in to the proposed activity and is fully informed as to what they are consenting to and any non-obvious consequences of giving or refusing that consent. Consent shall not be assumed as being given if no response has been received e.g. a consent form has not been returned. Where consent is being obtained for the collection or use of children's information, consent shall be obtained from a parent or guardian until the child reaches the age of 12. Consent shall be obtained directly from children aged 13 years and over where those children are deemed by the Trust to have sufficient maturity to make the decision themselves (except where this is not in the best interests of the child. In such cases, consent will be obtained from an adult with parental responsibility for that child).

5.2.8 The Trust shall ensure that where consent is obtained, there is a record of this. Where possible, consent shall be obtained in writing. All forms requesting consent shall include a statement informing the person of their right to withdraw, and an email address so they may notify the Trust of any changes or withdrawal of consent.

5.2.9 Fairness and transparency

5.2.10 The Trust shall be fair, open, and transparent in the way it handles personal data, and will publish privacy notices which explain:

- What personal data the Trust processes and why
- What our lawful basis is when we process that data
- Who we might share that data with
- If we intend to transfer the data abroad
- How long we keep the data for
- What rights data subjects have in relation to their data
- Who our Data Protection Officer is and how to contact them

5.2.11 The Trust's privacy notices shall be clear, concise, easily accessible and published on the Trust's website www.plymouthcast.org.uk/web. All forms collecting personal data shall include reference to the Trust's privacy notices and a link provided to their location.

5.3 Purpose limitation

5.3.1 The Trust shall collect personal data for specified (i.e. as described in the Trust's privacy notices), explicit and legitimate purposes and shall not process this data in any way which could be considered incompatible with those purposes (e.g. using the data for a different and unexpected purpose).

5.4 Data minimisation

5.4.1 The Trust shall ensure the personal data it processes is adequate, relevant, and limited to what is necessary for the purpose(s) for which it was collected.

5.5 Accuracy of data

5.5.1 The Trust shall take all reasonable efforts to ensure the personal data it holds is accurate and where necessary kept up to date. Where personal data is found to be inaccurate this information will be corrected or erased without delay.

5.5.2 The Trust will send frequent reminders, on at least an annual basis, to parents/carers, pupils, and employees, to remind them to notify the Trust of any changes to their contact details or other information.

5.5.3 The Trust shall carry out periodic sample checks of pupil and employee files containing personal data, to ensure the data is accurate and up to date.

5.6 Storage limitation and disposal of data

5.6.1 The Trust shall keep personal data for no longer than is necessary for the purpose(s) of the processing. The Trust shall maintain and follow a Record Retention Schedule, which sets out the timeframes for retaining personal data. This schedule shall be published alongside the Trust's privacy notices on the website.

5.6.2 The Trust shall designate responsibility for record disposal/deletion to nominated employees, who shall adhere to the Trust's Record Retention Schedule and ensure the timely and secure disposal of the data.

5.7 Security of personal data

5.7.1 The Trust shall have appropriate security in place to protect personal data against unauthorised or accidental access, disclosure, loss, destruction, or damage. This will be achieved by implementing appropriate technical and organisational security measures.

5.8 Technical security measures

5.8.1 The Trust shall implement proportionate security measures to protect its network and equipment and the data they contain. This includes, but is not limited to:

- having a Firewall, anti-virus, and anti-malware software in place
- applying security patches promptly
- restricting access to systems on a 'need to know' basis
- enforcing strong password policies; passwords shall be a minimum of 8 characters in length; changed at appropriate intervals and not shared or used by others
- encrypting laptops, USB/memory sticks and other portable devices or removable media containing personal data
- regularly backing up data
- regularly testing the Trust's disaster recovery and business continuity plans, to ensure data can be restored in a timely manner in the event of an incident
- use of two factor authentication (2FA) on accounts containing sensitive data

5.9 Organisational security measures

5.9.1 The Trust will ensure the following additional measures are also in place to protect personal data:

- Employees shall sign confidentiality clauses as part of their employment contract.
- Data protection awareness training shall be provided to employees during on-boarding and annually thereafter.
- Cyber security training, guidance or advice shall be cascaded to employees on a regular basis.
- Policies and guidance shall be in place relating to the secure handling of personal data whilst in school/Trust offices and when working remotely outside of these premises. These will be communicated to employees and other individuals as necessary, including policy revisions.
- Data protection compliance shall be a regular agenda item in governing body and Senior Leadership Team meetings.
- Cross cutting shredders and/or confidential waste containers will be available on the Trust's premises and used to dispose of paperwork containing personal data.
- Appropriate equipment and guidance will be available for employees to use and follow when carrying paperwork off Trust premises.

- The Trust's buildings, offices, and where appropriate classrooms shall be locked when not in use.
- Paper documents and files containing personal data shall be locked in cabinets/cupboards when not in use, and access restricted on a need-to-know basis.
- Procedures shall be in place for visitors coming onto the Trust's premises. These will include signing in and out at reception, wearing a visitor's badge and being escorted by a Trust employee (unless the visitor holds a valid Disclosure and Barring Service certificate, or it is otherwise appropriate for the person not to be escorted).
- The Trust shall have procedures in place to identify, report, record, investigate and manage personal data breaches in the event of a security incident.

5.10 Rights of Data subjects

5.10.1 Data subjects have several rights under the data protection legislation. The Trust shall respond to all valid requests (written or verbal) from data subjects exercising their rights without delay, and within one month at the latest.

5.10.2 Data subjects have the right to:

- Be informed about the use, sharing and storage of their data
- Request access to the personal data the Trust holds about them
- Have inaccurate or incomplete data corrected
- Ask for their data to be deleted when it is no longer needed
- Restrict the use of their data in certain circumstances
- Port (transfer) their data to another organisation in certain circumstances
- Object to the use of their data in certain circumstances (this includes direct marketing)
- Prevent automated decisions being taken about them (including profiling)
- Raise a concern with the Trust about the handling of their personal data. If they remain dissatisfied with Trust's response, they have the right to escalate this to the Information Commissioner's Office.

5.11 Handling requests

5.11.1 Data subjects exercising their data protection rights are recommended to put their request in writing and send it to the Trust at Edmund Rice Building, St Boniface College, Boniface Lane, Manadon Park, Plymouth, PL5 3AG. Data subjects can also exercise their rights verbally. Data Protection Requests shall be handled in line with the Trust's Data Protection Request Handling Procedure.

5.12 Data protection by design and default

5.12.1 The Trust shall have appropriate technical and organisational measures in place which are designed to implement the data protection principles in an effective manner, and will ensure that by default, it will only process personal data where it is necessary to do so. The Trust's Data Protection Policy and supplementary policies, procedures and guides explain how the Trust aims to achieve this.

5.13 Joint controller agreements

5.13.1 The Trust shall sign up to agreements with other data controllers where personal data is shared or otherwise processed on a regular basis, where it is necessary to do so.

5.14 Data processors

5.14.1 The Trust shall carry out due diligence checks with prospective data processors (e.g. suppliers providing goods or services which involve the processing of personal data on the Trust's behalf) to assess they have appropriate technical and organisational measures that are sufficient to implement the requirements of the data protection legislation and to protect the rights of data subjects.

5.14.2 Due diligence checks on prospective data processors shall be carried out alongside the Data Protection Officer. A record shall be kept of the Trust's findings.

5.14.3 The Trust shall ensure there are appropriate written contracts/Terms of Service in place with data processors, which contain the relevant clauses listed in Article 28 of the UK GDPR.

5.15 Record of processing activities

5.15.1 The Trust shall maintain a record of its processing activities in line with Article 30 of the UK GDPR. This inventory shall contain the following information:

- Name and contact details of the Trust and its Data Protection Officer
- Description of the personal data being processed
- Categories of data subjects
- Purposes of the processing and any recipients of the data (including data processors)
- Information regarding any overseas data transfers and the safeguards around this
- Retention period for holding the data
- General description of the security in place to protect the data

5.15.2 This inventory shall be reviewed annually and made available to the Information Commissioner upon request.

5.16 Management of personal data security breaches

5.16.1 The Trust shall follow the Personal Data Breach Handling Procedure in the event of a personal data security breach. These include incidents resulting in the:

- unauthorised or accidental disclosure or access to personal data
- unauthorised or accidental alteration of personal data
- accidental or unauthorised loss of access or destruction of personal data

5.16.2 All personal data security breaches and suspected breaches must be reported to the Data Protection Officer immediately, via the Trust's Data Protection Link Officer, by emailing admin@plymouthcast.org.uk or telephone 01752 977322.

5.16.3 All incidents will be recorded in the Trust's data breach log and investigated by a member of the Senior Leadership Team (or other person as appropriate), under the support and direction of the Trust's Data Protection Officer.

5.16.4 Notification to the ICO and Data Subjects

5.16.5 The Data Protection Officer shall determine whether the Trust must notify the Information Commissioner's Office and data subjects.

5.16.6 Where a breach is likely to result in a risk to the data subject, for example if they could suffer damage, discrimination, disadvantage, or distress as a result of the breach, the Data Protection Officer shall notify the Information Commissioner's Office (ICO), within 72hrs of the Trust becoming aware of the breach.

5.16.7 If the breach is likely to result in 'high risks' to data subjects, for example if the breach could lead to identity theft, psychological distress, humiliation, reputational damage or physical harm, the Trust shall inform the data subject promptly and without delay.

5.16.8 When informing a data subject of a personal data breach involving their personal data, the Trust shall provide in clear, plain language the:

- nature of the incident
- name and contact details of the Data Protection Officer
- likely consequences of the breach
- actions taken so far to mitigate possible adverse effects

5.17 Data Protection Impact Assessments

5.17.1 The Trust shall carry out Data Protection Impact Assessments (DPIAs) on the processing of personal data where this is likely to result in high risks to the rights and freedoms of data subjects.

5.17.2 The UK GDPR sets out three types of processing which will always require a DPIA:

- Systematic and extensive evaluation or profiling of individuals
- Large scale use of sensitive data
- Systematic monitoring of a publicly accessible area on a large scale

5.17.3 The Trust shall follow the Information Commissioner's Office supplementary list of processing, which also requires a DPIA:

- Use of innovative technology
- Denial of a service, opportunity, or benefit
- Large scale profiling
- Processing of biometric or genetic data
- Data matching
- Invisible processing
- Tracking
- Targeting children or other vulnerable individuals
- Risk of physical harm

5.17.4 The Trust shall also consider the European guidelines (Guidelines on Data Protection Impact Assessment), to help identify other likely high-risk processing, which includes:

- Use of sensitive data or data of a highly personal nature.
- Data concerning vulnerable data subjects.
- Innovative use or applying new technological or organisational solutions.

5.17.5 The results from DPIAs shall be recorded and shared with the Data Protection Officer, who will advise on any privacy risks and mitigations that can be made to reduce the likelihood of these risks materialising. The Data Protection Officer will monitor the outcome of the DPIA to ensure the mitigations are put in place. DPIAs shall be reviewed on an annual basis.

5.18 Data sharing

5.18.1 The Trust shall adhere to the statutory and non-statutory guidance around sharing personal data, as set out in the:

- Department for Education: Keeping Children Safe in Education (2021)
- Information Commissioner Office: Data Sharing Code of Practice (2020)
- HM Government: Information Sharing Advice for Practitioners providing safeguarding services to children, young people, parents, and carers (2018)

5.18.2 When sharing personal data with third parties the Trust shall adhere to the following principles:

- Data subject(s) shall be made aware of the sharing through privacy notices or specific communications regarding the sharing
- An appropriate lawful basis shall be identified prior to the sharing
- Data shared shall be adequate, relevant, and limited to what is necessary
- Accuracy of the data shall be checked prior to the sharing (where possible)
- Expectations regarding data retention shall be communicated
- Data shall be shared by secure means and measures in place to protect the data when received by the third party
- A record shall be kept of the data sharing.

5.18.3 The Trust recognises that the data protection laws allow organisations to share necessary personal data with third parties to protect the safety or well-being of a child and in urgent or emergency situations to prevent loss of life or serious physical, emotional or mental harm.

5.19 Appointment of a Data Protection Officer

5.19.1 The Trust shall appoint a Data Protection Officer to oversee the processing of personal data within the Trust, in compliance with Articles 37-38 of the UK GDPR. This person shall be designated on the basis of professional qualities and in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39 of the UK GDPR.

5.19.2 The Trust shall publish the contact details of the Data Protection Officer and communicate these to the Information Commissioner’s Office.

6 Policy history

Policy Version and Date	Summary of Change	Amended by	Implementation Date
Version 2.1 July 22	This policy replaces the Trust's existing Data Protection Policy	Data Protection Officer	01.09.2022

Appendix 1
Data Protection Policy Definitions

Term Used	Summary Definition
Personal data	Personal data means any information relating to an identified or identifiable living individual. This includes a name, identification number, location data, an online identifier, information relating to the physical, physiological, genetic, mental, economic, cultural, or social identity of that individual.
Special categories of personal data	Special categories of personal data mean personal data which reveal the racial or ethnic origin, political opinions, religious or philosophical beliefs and the trade union membership of the data subject. It also includes the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health, and data relating to an individual's sex life or sexual orientation.
Processing	Processing means any operation or set of operations which is performed on personal data, such as the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
Data subject	An identifiable, living individual who is the subject of personal data.
Data controller	A data controller is an organisation who determines the purposes and means of the processing of personal data.
Data processor	A data processor is an organisation who processes personal data on behalf of a data controller, on their instruction.