

Plymouth CAST

Multi Academy Trust, Diocese of Plymouth

Data Protection Policy

Guidance on the application of this policy can be obtained from Plymouth CAST HR

Email: Personnel@plymouthcast.org.uk

Tel: 01364 645450

1. **Purpose**
   1. Plymouth CAST Multi-Academy Trust and its member schools (CAST) handle and process information relating to individuals (e.g. employees, pupils, parents etc.) while conducting its day-to-day educational activities.
   2. According to the Charter of Fundamental Rights of the European Union, every individual has the right to the protection of any information that concerns him or her. The European Union has passed the General Data Protection Regulation (GDPR) (on the protection of natural persons with regard to the processing of personal data) to harmonise the implementation of such right within the EU. The UK has formally adopted this regulation. Accordingly, the GDPR imposes strict obligations on CAST that are designed to safeguard the rights of individuals in relation to the handling of their information (or Personal Data).
   3. The purpose of this policy is to ensure that CAST carries out its activities in accordance with applicable personal data protection regulations (including the GDPR) so that everyone’s fundamental right to data protection is duly preserved, guaranteed and respected.
   4. CAST has appointed a Data Protection Officer (DPO) with overall responsibility for compliance with these regulations in order to oversee the operation of this policy and to discharge the legal obligations of the Trust. It has also appointed a Data Protection Coordinator (DPC) within each school, who is accountable to the CAST DPO for ensuring that their school complies with the requirements of this policy. It is the responsibility of all Employees to know the identity of their respective DPC.
   5. It is the responsibility of the head of each department and/or the Principal of each school to ensure that their staff are aware of, and comply with, the requirements set out in this policy.
   6. It is the responsibility of the CAST DPO and the school DPCs to organise the training necessary for employees to comply with the requirements of this policy.
2. **Scope**
   1. This policy applies to all directors, employees and members of Local Governing Boards of CAST, together with contractors and agency workers who are subject to the conditions and scope of this policy. It also applies to all parents/carers of pupils who attend CAST schools. If you process or use Personal Data or supervise staff involved in these activities you must ensure that you follow the requirements of this policy at all times.
   2. The policy applies to all Processing of Personal Data.
   3. Where appropriate, this policy should be read in conjunction with the CAST Freedom of Information Policy.
   4. A breach of this policy represents serious misconduct and may result in an internal investigation as well as disciplinary action being taken up to and including termination of employment.
3. **Definitions**
   1. **Authorised Locations:** A place approved by the DPO for the storage of Personal Data.
   2. **Data:** See Personal Data and Sensitive Personal Data below.
   3. **Data Access Request (SAR):** A formal request to CAST or one of its subsidiaries from a Data Subject to access their Personal Data. These should be in writing and CAST have a limited time period under law to respond to them.
   4. **Data Subject:** The individual to whom the Personal Data relates.
   5. **Direct Marketing:**  Any communication by whatever means of any advertising or marketing material that is directed to particular individuals. This will include any materials sent by mail, electronic communications, telephone or fax.
   6. **Employee:** Anyone employed by CAST and anyone engaged by contract whose role includes any of the activities that could be carried out by and employee.
   7. **External Data Processors:** Third party organisations or individuals that are contracted to provide CAST with personal data processing. These can include:
      1. Payroll and management of employees
      2. Data archiving/destruction
      3. Website hosting services
      4. Data screening, mailing house services and other marketing support services
      5. Courier and despatch services
      6. Confidential waste destruction
      7. Business or operational administration
      8. Any outsourcing activity
   8. **Parent:** Includes carers and anyone who exercises parental responsibilities over a pupil.
   9. **Personal Data:** Any data that relates to and can, whether on its own or in conjunction with other information, specifically identify an individual living person. Personal data includes, for example, names and addresses, e-mail addresses, IP addresses, recruitment details etc. It also includes opinions about individuals as well as facts and also applies to corporate contacts.

Personal data includes data held electronically on a computer or network and data held in hard copy paper format including, for example, on microfiche, hand held devices, mobiles, laptops, databases, filing cabinets or visitors books.

* 1. **Processing:** This is a wide ranging term that, in practice, covers any use of Personal Data including:
     1. Obtaining, recording, holding, and carrying out any operation(s) on the Personal Data.
     2. Organisation or alteration of the Personal Data
     3. Retrieval, disclosure or use of the Personal Data

All such data processing activities will constitute Processing within the meaning of data protection laws.

* 1. **Sensitive Personal Data:** Any information about or pertaining to an individual’s genetic or biometric data, physical or mental health, racial or ethnic origin, sexual life, politics, religion, trade union membership, or any information about alleged or committed criminal offences.
  2. **Storage:** The place where Personal Data and Sensitive Data is kept. This includes all means of physical, electronic, recorded and other mechanisms for Data capture.

1. **Policy**
   1. **Responsibility:** The Chief Executive Officer (CEO) has overall responsibility for the operation of this policy within CAST. Principals have responsibility for the operation of this policy within their schools. The designated CAST Data Protection Officer (DPO) reports directly to the CEO. School DPO’s have a functional or ‘dotted line’ accountability to the CAST DPO.
   2. **Principles**

When collecting and processing personal data, employees shall make sure that such personal data conform to the following principles that require that personal data must be:

* + 1. processed in a lawful, fair and transparent manner (***Principle of Lawfulness***);
    2. collected for specified, explicit and legitimate purposes (***Principle of Specified Purpose***);
    3. appropriate, relevant and limited to the minimum required as regards the purposes for which they are processed (***Principle of Concision***);
    4. accurate, and kept updated (***Principle of Accuracy***);
    5. preserved in a manner serving to identify the Data Subject for a period no greater than required for the purposes for which they are processed (***Principle of Temporariness***); and
    6. processed in a manner that guarantees appropriate security of the personal data, including protection against unauthorised or unlawful processing and against the loss, destruction or accidental damage thereof, by means of the application of appropriate technical or organisational measures (***Principle of Integrity and Confidentiality***)
  1. **Principle of Lawfulness (Personal Data must be collected and processed in a fair, transparent and lawful manner).** CAST must have a “lawful” reason for collecting data (i.e. a legal obligation, a contract with – or for the benefit of – the Data Subject, or the Data Subject’s consent).

**Sensitive Personal Data:** Employees must not process or store sensitive personal data unless this is necessary and then only if the Data Subject has explicitly consented. A record of that consent must be retained and be available for inspection for at least two years after the Sensitive Personal Data is no longer being processed or stored.

* 1. **Principle of Specified Purpose (Personal Data are collected for specific, explicit and legitimate purposes only).** CAST must ensure the data is only used for the purpose for which it was collected and that such purpose is:
* **Specific**: it does not allow for multiple unrelated uses;
* **Explicit**: it has been conveyed to the Data Subject upon collection;
* **Legitimate**: it is connected with the educational activities of CAST.

Any personal data collected for a specific purpose may not be subsequently processed for a different purpose. Should it prove necessary to radically change the purpose for which the personal data in question were collected, the Employee will be required to inform the Data Subject of the change in question beforehand.

* 1. **Principle of Concision (Personal Data are appropriate, relevant and limited to the minimum required as regards the purposes for which they are processed).** This principle requires data minimisation. CAST must only collect and process personal data that are required to complete a specific purpose.

**Quality:** All processing of personal data must be adequate, relevant and not excessive for the specific purposes for which the data was obtained. The most appropriate time for informing the Data Subject with notice of the purposes of collection is at the time the personal data is collected.

* 1. **Principle of Accuracy (Personal Data are accurate and up-to-date).** CAST must ensure the personal data they collect and process is free from error and of a relevant time frame.

**Accuracy**: Personal data must be kept accurate and up to date, and must be adequate, relevant and not excessive. Reasonable steps must be taken to ensure the accuracy and quality of personal data, and to prevent it from becoming out of date. Periodic reviews of the information held should be completed to ensure on-going accuracy. If data is found to be out of date or inaccurate, it must be corrected as soon as is reasonably possible.

**Inaccurate Information:** Data Subjects have the right to require that CAST correct any inaccurate data held about him or her. CAST is legally required to respond to such a request within 21 days of receiving it. Any requests for inaccuracies to be corrected must be immediately forwarded to the CAST DPO in the first instance, who will determine who is best placed to make the correction. CAST has a legal obligation to comply with such requests provided that the Data Subject has been satisfactorily identified, and the employee should take reasonable steps to identify the Data Subject before forwarding the request to the DPO.

Rights to correct information include:

* Amendment
* Erasure
* Destruction
* Blocking
  1. **Principle of Temporariness (Personal Data must not be kept for no longer than is necessary).** Employees ofCAST must abide by the local data retention policies.
  2. **Principle of Integrity and Confidentiality (Personal Data are held securely).** This principle demands that CAST takes sufficient technical and organisational measures to ensure that personal data is kept secure. This includes the physical security of the hardware and software, staff awareness and training and the development of adequate polices and processes.

**Authorised Locations:** Personaldata must only be stored at authorised locations

**Data Security:** Personal Data must be stored and managed securely and all Employees must take precautions against physical loss or damage. They must also ensure that both access to and disclosure of personal data is restricted as appropriate. In particular:

Personal data must not be disclosed, either orally or in writing or otherwise, to an unauthorised third party without a clear “need to know” reason being identified prior to disclosure and in accordance with the notice provided to the Data Subject.

When physical personal data is left unattended, it must be secured – for example within locked office furniture. Personal Data in electronic form must be inaccessible when left unattended.

Files containing personal data must not be left in open view.

Files containing personal data stored and processed in the systems of CAST must be protected by authentication systems approved by the Board.

Personal data stored on laptop computers and mobile phones are subject to the provisions of this policy.

Principals and managers have the responsibility for ensuring that staff are aware of the restrictions for accessing personal data within their area and also for observing the information security policies, procedures and related guidance of CAST.

**Unauthorised Access:** Accessing, deleting, or otherwise using any information which is not part of an employee’s duties or without prior authority is a serious disciplinary offence.

* 1. **Overseas transfer of data** A number of restrictions on personal data transfer across borders and outside of the European Economic Area (EEA) apply. No personal data transfers outside the EEA may be undertaken without being authorised by the CEO.
  2. **Rights of the Data Subject** CAST must ensure the rights of Data Subject must be observed and employees must take all reasonable steps to ensure that they are aware of and respect these rights. These rights include:
     1. **To be informed-** The right to be told how and why CAST is collecting their data, how it is used and who it is being shared with. Subject to certain conditions, CAST is also required to inform the Data Subject if their data is involved in a data breach. Data Subjects must be provided with at least the following information:

1. the identity and the contact details of CAST as the controller of the personal database;
2. the purposes for which their Personal Data will be processed;
3. the period during which their Personal Data will be retained;
4. the existence of the right to request access to their Personal Data, and the rectification, cancellation or objection to the Processing of the Personal Data;
5. the recipients or categories of recipients of their Personal Data;
6. any other information that might be necessary in accordance with the specific circumstances in which their Personal Data are gathered;
7. if the provision of data is mandatory or voluntary, and any possible consequences following from the Personal Data not being provided; and
8. the source from which the Personal Data are derived, if they were not obtained from the Data Subject him/herself.
   * 1. **Of access**- Data Subjects have the right, subject to certain exceptions and procedural requirements, to access Personal Data that is being processed about him or her, through the means of a Data Access Request.

CAST is required by law to respond to such a Request within 1 calendar month. Any Employee receiving a Data Access Request must immediately forward it to the CAST DPO.

Under no circumstances should an employee respond to a Data Access Request

A Data Access Request may be received in any number of forms, including a telephone call, email or letter. In the case of a telephone call, the Data Subject should be requested to submit the Data Access Request in writing to the DPO. The DPO should be notified of the request and of your response.

* + 1. **Of rectification-** The right to demand that any data held on him or her that is inaccurate or incomplete is rectified.
    2. **Of erasure-** Known as the right to be forgotten, CAST must ensure the deletion or removal of personal data when the data subject can demonstrate there is no compelling reason for its continued processing.
    3. **To restrict processing-** If a data subject asks for processing to be restricted, CAST is permitted to store the personal data, but not further process it. CAST must retain the minimum amount of information to ensure that the restriction is respected in the future.
    4. **Data portability-** The right to move personal data, held in an electronic format, from one environment to another.
    5. **To object-** CAST must observe a data subject’s choice to object to their data being used for direct marketing.
    6. **To object to** **automated decision making and profiling**- CAST must respect a data subjects right to object to automated decisions **–** individuals can request that decisions made about them by automatic means be retaken manually.
  1. **Rights to process Employee Data:** It is the responsibility of the DPO to ensure that processes are in place to obtain the consent from individual employees to process their personal data. Any requirement to process sensitive personal data must be first approved by the CEO.
  2. **Processing parent and pupil data:** It is the responsibility of each Principal to obtain the written consent from the parent to process each pupil’s personal data together with the personal data of the parent insofar as it relates to the well-being of the pupil.
  3. **Documentation and Processing Requirements:** It is the responsibility of the CAST DPO to issue procedures, require the use of standard form documentation and establish suitable controls to ensure that the requirements of this policy are followed.
  4. **Data Breach Plan:** It is the responsibility of the CAST DPO to develop and implement a Data Breach Response Plan and to communicate it to all relevant personnel. The plan must be approved by the Board and reviewed on an annual basis. All breaches must be reported to the CEO and the Board, together with recommendations as to the appropriate actions.
  5. **Subject Access Requests:** It is the responsibility of the CAST DPO to develop and implement a Subject Access Response Plan to ensure that all SARs are addressed in the legally required period of time. A list of all SARs and the responses provided must be reviewed and approved by the CEO at the end of each quarter.
  6. **Certification:** Each Principal and School DPO must provide an annual written certification to the CAST DPO that the requirements of this policy are being followed in their school and that all breaches have been reported to the CAST DPO. The CEO and the CAST DPO must provide an annual written confirmation to the Board that the requirements of this policy have been followed across CAST and that all breaches have been reported to the Board.

1. **Reporting Non Compliance**

Employees who know or suspect that this policy may have been violated must immediately notify their Principal or Manager **and** the CAST DPO. Alternatively, if they believe that the matter is sufficiently serious, they may contact the CAST Hotline.

1. **Consequences of Non Compliance**

Employees who violate this policy are subject to disciplinary action, up to and including termination of employment. Business partners who violate the applicable parts of this policy are subject to termination of all commercial relationships with CAST and may be reported to the Information Commissioners Office.