Data Protection Request Handling Procedure 2025-2026

Approved by:	SELT
Date:	22.09.25
Version:	5
Review Date:	September 2026

This procedure shall be followed by employees responsible for handling requests made under the UK General Data Protection Regulation 2016 (the UK GDPR) and the Data Protection Act 2018. It supports the school's Data Protection Policy, which should be read alongside this.

This procedure does not relate to requests made under the Freedom of Information Act 2000, which is governed by separate procedures.

Queries about this procedure should be addressed to the school's Data Protection Officer, (Firebird Data Protection Consultancy) Email: dpo@firebirdltd.co.uk

Contents

1. Introduction

This procedure explains how Plymouth CAST handles data protection requests in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (the data protection legislation). It applies to requests from any individual whose personal information the school/Trust may hold. This includes pupils, parents and carers, staff members (including temporary and agency workers), governors and trustees, job applicants, volunteers, visitors, and anyone who has contacted the school/Trust to make an enquiry, complaint, or request.

2. Data protection rights

Under the data protection legislation, individuals (known as data subjects) have a range of rights in relation to their personal data. These rights include the right to be informed about how their information is used, the right to access their data (Subject Access Requests), and the right to have inaccurate or incomplete information corrected. In some circumstances, they may also have the right to request their data is deleted, to restrict or object to its processing, or to receive their data in a portable format so it can be shared with another organisation.

In addition, data subjects can object to their information being used for direct marketing purposes or tasks carried out in the public interest. They also have the right not to be subject to decisions made solely by automated means (including the use of artificial intelligence tools), where this could have a significant effect on them.

3. Making a data protection request

Anyone wishing to exercise their rights should make a data protection request. Requests may be made in writing or verbally, and should be directed to the school via the school's published contact email and/or postal addresses or to the Trust by email to admin@plymouthcast.org.uk or addressed to The Chief Operating Officer, Plymouth CAST, Edmund Rice Building, St Boniface College, Boniface Lane, Manadon Park, Plymouth, PL5 3AG. If a verbal request is received, for example during a telephone call or in person, the nominated staff member will summarise the request in writing and ask the individual to confirm that this summary is accurate. The school/Trust will also make reasonable adjustments for those who need additional support to make a request, in line with the school/Trust's duties under the Equality Act 2010.

It is important to note, that requests do not need to mention the words "data protection" or "UK GDPR" in order to be valid. Staff should therefore remain alert to any correspondence that may amount to a data protection request

4. Logging and acknowledging requests

Once a request is received, schools should inform the Trust's Chief Operating Officer who will record it in the Trust's Information Request Log. An acknowledgement shall then be sent to the requester, using the school/Trust's template response letters. Where there is any doubt about the identity of the requester, the school/Trust may ask for proof of identity such as a passport, driving licence, or utility bill.

If the request has been made on behalf of another person, such as by a solicitor or a family member, then evidence of their entitlement to receive the data must be provided. This may include written consent from the individual concerned, a copy of a power of attorney, or a court order. Where there is uncertainty, the matter will be referred to Plymouth CAST's Data Protection Officer for advice.

5. Timescales and fees

The school/Trust is required to respond to data protection requests without undue delay and, in any event, within one calendar month of receipt. If the following month is shorter, the response date will fall on the final day of that month, or on the next working day if that date is a weekend or public holiday.

The timescale begins on the day the request is received, unless further clarification or proof of entitlement is required, in which case the clock will start once this information is provided. For particularly complex requests, or if an individual has made a number of requests at the same time, the school/Trust may extend the deadline by up to two further months. If this happens, the requester shall be notified within the first month, and the reasons for the extension explained.

Normally, the school/Trust cannot charge a fee for dealing with a request. However, if a request is considered to be "manifestly unfounded" or "manifestly excessive", the school/Trust may either refuse to comply with it or charge a reasonable administrative fee. A fee may also be charged if the individual asks for additional copies of information that has already been provided.

6. Assessing manifestly unfounded or excessive requests

The legislation gives the school/Trust discretion to refuse or limit requests that are manifestly unfounded or excessive. This might include situations where a request is clearly intended to cause disruption or harass the school/Trust; where repeated requests are made without sufficient time having passed; or where there is significant overlap with other requests. The

school/Trust will document its reasoning carefully in such cases and will seek advice from Plymouth CAST's Data Protection Officer before refusing a request or charging a fee.

7. Actioning requests

Once a request has been logged and acknowledged, the responsible staff will contact relevant staff, governors, or trustees to identify whether the requested information is held and, if so, where it is stored. Reasonable searches of both electronic and paper records will be carried out. Staff are expected to cooperate fully and promptly with such searches.

If the school/Trust does not hold the requested information, or if there are lawful grounds to withhold it, the requester will be informed in writing within the statutory timeframe.

8. Subject access requests (SARs)

Requests from pupils

Pupils themselves are entitled to request access to their own personal data, provided they have the maturity to understand their rights. The Information Commissioner's Office suggests, in most cases, it is reasonable to assume that pupils aged 12 years or over have sufficient maturity, unless there is evidence to the contrary.

Where a pupil does not have sufficient maturity, or where disclosure directly to them would not be in their best interests, the request should be made by a parent or carer acting on their behalf.

Requests from parents or carers

Parents or carers who have parental responsibility may request access to their child's personal data in certain circumstances:

- Where it is routine information they would usually receive as a parent; or
- Where the child consents (if they are sufficiently mature); or
- Where disclosure is clearly in the child's best interests.

The school/Trust shall decide on a case-by-case basis whether it is necessary and appropriate to discuss a request made by a parent with the pupil, prior to releasing their records. The school/Trust shall consider the validity of any consent received from a child (under 18 years old). Consent shall only be accepted where the child is fully informed and understands what they are consenting to, and it is freely given (eg not coerced by the parent).

9. Exemptions

There are situations where the school/Trust is not obliged to provide the information requested, i.e. where an exemption applies. For example, the school/Trust is not permitted to disclose personal information about someone else without their consent, unless it is reasonable to do so.

Information may also be withheld if its disclosure would cause serious harm to someone's mental or physical health, prejudice the prevention or detection of crime, breach legal professional privilege, or another law prohibits the disclosure.

Other exemptions may apply to references provided in confidence, exam scripts or results prior to official release, and management information where disclosure could prejudice the school/Trust's operations. In all cases, decisions to withhold information will be carefully considered, advice shall be sought from Plymouth CAST''s Data Protection Officer and redactions made where necessary.

10. Preparing and disclosing information

Where an exemption applies, the relevant sections of documents will be securely redacted before disclosure. Redaction will be carried out using appropriate software (such as Adobe Professional) or, for paper copies, by permanently obscuring the text so that it cannot be read.

If the records include correspondence from external professionals, such as police officers or health practitioners, the school/Trust will, wherever possible, consult with the relevant professional or their Data Protection Officer prior to release, unless it is evident that the requester has already received a copy of the correspondence or documentation.

Before disclosure, the material will be reviewed by a second colleague to ensure it falls within the scope of the request and that all necessary redactions have been correctly applied. A record of the disclosure, including both redacted and unredacted versions, will be securely retained in case of a subsequent complaint or challenge.

Information will be provided in the format requested, or in a format reasonably expected by the requester. Typically, this will mean supplying either a physical copy or an electronic copy by email. Where information is sent electronically, the school/Trust will use a secure encrypted service.

If the requester specifically asks for the information to be sent via unencrypted email, they will first be advised that this method is not recommended due to security risks. Should they still wish to proceed, the school/Trust will comply once written confirmation has been received.

If a physical copy is requested, the disclosure may be:

- handed directly to the requester
- collected from the school/Trust by arrangement; or
- posted using Royal Mail Special Delivery (standard post will not be used for sensitive or confidential information).

Alongside the disclosure, the requester is also entitled to receive supplementary information about how the school/Trust processes personal data. This information is set out in the Trusts

privacy notices, and a link to these notices shall be provided in the Subject Access Request response letter.

The case handler shall complete the Subject Access Request Disclosure Checklist and keep this on file along with a copy of the disclosure (electronic or paper). The Chief Operating Officer must be informed when the request has been completed, and will then update the Information Request Log to show that the request has been closed.

11. Complaints

Data subjects have a legal right to make a complaint if they are dissatisfied with how their request or personal information has been handled by the school/Trust. Where concerns cannot be resolved informally, applicants shall be directed to make a formal complaint through the Trust's formal complaints procedure.

If the applicant is not satisfied with the outcome of their formal complaint, they can escalate this to the Information Commissioner's Office (ICO) by email at casework@ico.org.uk, or by post at Customer Contact, Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, SK9 5AF. They also have the right to pursue their complaint through the courts.

Appendix A: Summary of Changes

This appendix summarises the key changes made between Versions 4 and 5 of the Data Protection Request Handling Procedure. It should be read alongside the updated policy to provide clarity on what has been revised, streamlined, or newly introduced.

Scope and Introduction
V5 includes a new Introduction section with clearer scope, listing pupils, parents, staff (including agency), governors, trustees, volunteers, visitors, job applicants, and enquirers.

Terminology
V4 referred to the Trust only. V5 refers to 'school/Trust' throughout to emphasise applicability at both levels.

Structure and Layout
V4 had 7 main sections. V5 expanded to 11 sections, including new sections on Assessing manifestly unfounded requests, Exemptions, and Preparing & disclosing information.

Data Protection Rights
V4 listed rights in detail with examples of data subjects. V5 simplified wording but covers same rights (informed, access, rectification, erasure, restriction, portability, objection, automated decisions/AI).

Making a Data Protection Request
V4 requests directed only to Trust (COO). V5 allows requests to schools or Trust; verbal requests handled by nominated staff; stronger emphasis on reasonable adjustments under Equality Act.

Logging and Acknowledging Requests
V4 COO logged requests, used SAR templates. V5 schools notify COO, who records in Trust log, using school/Trust templates. More detail on proof of ID/entitlement and DPO referral.

Timescales and Fees
Core one-month response time remains. Both allow two-month extension for complex cases. V5 adds separate section on 'manifestly unfounded or excessive requests', requiring documented reasoning and DPO advice.

Manifestly Unfounded/Excessive Requests
V4 gave detailed examples (malicious, harassment, grudges, repeated). V5 gives shorter examples (disruption, harassment, repeated, overlapping) and requires recording justification.

Actioning Requests
V4 COO/Headteacher responsible. V5 broadens responsibility to relevant staff; emphasises cooperation and updating requester if data not held or refusal justified.

Subject Access Requests (SARs)
Both cover pupil maturity (ICO presumes 12+). V4 more detail on parental access limits and consent. V5 simplifies into 'Requests from pupils' and 'Requests from parents/carers'.

Exemptions
V4 long detailed list (third party, harm, crime prevention, legal privilege, forecasting, exams). V5 shorter higher-level list with DPO advice required.

Preparing and Disclosing Information
V4 highly detailed (redaction methods, Egress Switch, Special Delivery, external consultation, checklist). V5 condensed: mandatory second colleague review, retention of redacted/unredacted copies, COO updates log.

Complaints
V4: complain to responder or DPO, escalate via Trust complaints procedure, then ICO. V5: formal Trust complaints procedure, then ICO or courts (courts option is new).