



Data Protection Request Handling Procedure 2026-2027

Approved by:	SELT
Date:	22.09.26
Version:	6
Review Date:	September 2027

This procedure shall be followed by employees responsible for handling requests made under the UK General Data Protection Regulation (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 or the Environmental Information Regulations 2004, which are governed by separate procedures.

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

Contents

1. Scope.....	3
2. Data protection rights.....	3
3. Handling data protection requests.....	4
Recognising a request.....	4
Logging and acknowledging requests.....	4
Confirming identity.....	4
Requests made on behalf of another person.....	4
Timescales.....	5
Clarification.....	5
Time extension.....	5
Fees.....	6
Manifestly unfounded or excessive requests.....	6
Requests drafted using artificial intelligence (AI).....	6
Right to complain.....	7
4. Subject Access Requests (SARs).....	7
Right of access to personal data.....	7
Personal data.....	7
SARs involving children.....	7
Preserving relevant information.....	8
Conducting searches.....	9
Preparing the disclosure.....	9
Disclosure of staff names.....	10
Third party consultation.....	10
Redactions.....	10
Peer review and SAR disclosure checklist.....	11
Disclosure format.....	11
Disclosure letter and supplementary information.....	11
Secure disclosure.....	12
Retaining a copy and closing the SAR.....	12
5. Rectification Requests.....	12
6. Erasure Requests.....	13
7. Other data protection requests.....	14
Appendix A: Summary of Changes.....	16
1. AI-Assisted Requests (New Section).....	16
2. Statutory "Stop the Clock" Clarification Rules.....	16
3. Duty to Preserve Records.....	16
4. Standard for Searching Data Repositories.....	16
5. Presumption of Non-Redaction for Education Staff.....	17
6. Rectification Rules: Professional Opinions vs. Factual Errors.....	17
7. Document Structure & Layout.....	17

1. Scope

This procedure explains how Plymouth CAST and its schools handle 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 individuals exercising their data protection rights.

This includes pupils and students (current and former), parents and carers, employees (current and former), agency workers, governors, trustees, directors, volunteers, visitors, job applicants, and anyone else who has contacted Plymouth CAST or a school to make an enquiry, complaint or request.

2. Data protection rights

Individuals have a number of rights in relation to their personal data. These include:

- **Right to be informed** – know how and why we collect, use and share their personal data
- **Right of access** – request a copy of the personal data we hold about them
- **Right to rectification** – ask us to correct personal data that is inaccurate or incomplete
- **Right to erasure** – ask us to delete their personal data in certain circumstances
- **Right to restrict processing** – ask us to limit how we use their personal data in certain circumstances
- **Right to object** – to object to certain uses of their personal data, including direct marketing and in some circumstances processing carried out in the public interest
- **Right to data portability** – ask us to provide their personal data to them, or transfer it to another organisation, where this right applies
- **Rights relating to automated decision-making** – where significant decisions are made solely by automated means, to have appropriate safeguards in place, including the right to human intervention and to challenge the decision
- **Right to complain** – to complain to the school or Trust if they are unhappy with how their personal data or data protection rights have been handled.

Not every right applies in every situation. The School/Trust's response will depend upon the circumstances, the information concerned and the lawful basis for processing it.

3. Handling data protection requests

Recognising a request

When individuals exercise their data protection rights, this is called making a data protection request. A data protection request does not have to mention the UK GDPR or the individual's data protection rights.

Requests can be received in writing including by email, letter or through other communication channels used by the School, or verbally. Requests may also be directed centrally 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**. Reasonable adjustments should be made for individuals who require assistance in exercising their rights.

Logging and acknowledging requests

When a request is received, schools should inform the Trust's Chief Operating Officer. It shall be recorded in the Trust's Information Request Log. An acknowledgement shall then be sent to the requester, using the School/Trust's template acknowledgement letters.

Confirming identity

The School/Trust must be satisfied of the identity of the person exercising the right before releasing personal data or taking other action. Additional identification should only be requested where it is reasonable and proportionate to do so.

The School/Trust should not routinely request formal identification documents where the individual's identity is already known. 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.

Requests made on behalf of another person

An individual may authorise another person, such as a solicitor, advocate or family member, to exercise their data protection rights for them. The School/Trust must be satisfied that the representative has appropriate authority. Evidence might include:

- written authority from the individual
- a valid power of attorney
- an appropriate court order, or
- other satisfactory evidence of authority

Authority to act for someone does not automatically mean that every piece of information relating to them should be disclosed to that representative.

Any concerns about confidentiality, capacity, safeguarding or the person's wishes should be considered before responding to a data protection request. Where there is uncertainty, advice shall be sought from Plymouth CAST's Data Protection Officer and where relevant the Designated Safeguarding Lead.

Timescales

The School/Trust must respond to data protection requests without undue delay and normally within one calendar month. The response period usually begins when the request is received, although where reasonable identity checks or evidence of authority are required, it will not begin until sufficient information has been received.

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.

Clarification

Where clarification is reasonably required to understand a data protection request, the School/Trust may ask the requester for further information. This may be necessary where the request is unclear, very broad, covers a long period, or the School/Trust holds a large amount of information about the individual.

For a Subject Access Request, where clarification is reasonably required to identify the personal data or processing activities requested, the statutory response period may be paused while the School/Trust waits for that clarification. The clock stops on the day clarification is requested and resumes on the day after it is received.

The School/Trust may invite a requester to narrow a broad SAR, for example by identifying a particular period, incident, member of staff or category of records.

Clarification must not be used unnecessarily or to delay a response. The School/Trust should record when clarification, identity evidence or authority was requested and received, and calculate the deadline accordingly.

Time extension

When handling a Subject Access Request, the School/Trust must normally respond without undue delay and within one calendar month. The School/Trust may extend this period by up to a further two months where this is necessary because the request is particularly complex or the individual has made a number of requests, for example, requests relating to multiple family members.

The need for an extension must be considered on a case-by-case basis. If an extension is required, the requester must be informed (using the School/Trust's template Time Extension letter) within the original one-month period and told:

- that the deadline has been extended;

- the reason for the extension; and
- when they can expect to receive the School/Trust's response.

An extension must not be used simply because the School/Trust is busy, relevant staff are absent, it is a school holiday, or redacting the records will take time.

The School/Trust should keep a clear record of the original deadline, any period during which the clock was paused, the reason for any extension, and the revised response date.

Fees

Data protection requests will normally be handled free of charge. In limited circumstances, the School/Trust may refuse to comply with a request, or charge a reasonable fee for dealing with it, where the request is manifestly unfounded or excessive. In the case of a Subject Access Request, a reasonable fee may also be charged where the individual asks for further copies of personal data already provided. Any fee must be reasonable and reflect the administrative cost of dealing with the request.

Manifestly unfounded or excessive requests

The threshold for treating a request as manifestly unfounded or excessive is high. Relevant circumstances may include:

- Repeated requests for substantially the same information within an unreasonable period
- Requests forming part of a pattern that clearly demonstrates abuse of the right
- Significant overlap with previous requests
- Circumstances indicating that the request is being used maliciously with no genuine intention of exercising a data protection right.

A difficult, time-consuming or inconvenient request is not necessarily 'excessive'. The School/Trust must consider the particular circumstances and retain evidence supporting its decision.

Advice shall be obtained from Plymouth CAST's Data Protection Officer before refusing a request or charging a fee.

Requests drafted using artificial intelligence (AI)

Individuals may use AI tools to help draft a data protection request. This does not make the request invalid and it must be handled in the same way as any other request. AI-assisted requests may sometimes be unnecessarily broad, repetitive, unclear or contain inaccurate statements about the law or the individual's rights.

As good practice, the School/Trust shall:

- assess the request against the requirements of the UK GDPR rather than relying on legal assertions made in the request
- seek clarification where this is reasonably required to understand the scope of the request
- invite the requester to narrow an unnecessarily broad request where this would help identify the information or action the individual is likely to want, and
- consider repeated or substantially overlapping AI-assisted requests in the same way as other repeated requests

The use of AI must not, by itself, be treated as a reason to refuse a request, regard it as excessive or apply a different standard of handling.

Right to complain

Individuals have the right to complain to the School/Trust about how their data protection request has been handled. Complaints can also include concerns about the use, disclosure, accuracy, retention or security of personal data. Data protection complaints shall be handled under Plymouth CAST's Data Protection Complaints Handling Procedure.

4. Subject Access Requests (SARs)

Right of access to personal data

Article 15 of the UK GDPR gives an individual the right to obtain from the School/Trust:

- confirmation that the School/Trust is processing their personal data
- access to, including a copy of that personal data, and
- information about how and why their personal data is being processed

A Subject Access Request (SAR) is the way an individual exercises this right.

The right of access is to 'personal data', not to documents. The School/Trust is therefore not automatically required to provide every document, email or record in which the individual is named or referred to.

Personal data

Personal data is any information that relates to an identified or identifiable individual. This may include factual information, opinions, observations, decisions and correspondence about the person. Information can still be personal data even if the individual is not named, where they can be identified from the content or surrounding context.

SARs involving children

The UK GDPR rights apply equally to children as well as adults. This includes the right to access the personal data the School/Trust holds about them. The right of access belongs to the child, even where a parent, carer or other person exercises that right on their behalf. Parents and carers do not automatically have a right under the UK GDPR to access their child's personal data.

Where a child is sufficiently competent to understand and exercise their own data protection rights, they should normally make the SAR themselves or authorise a parent, carer or other person to act on their behalf.

As a general guide, the Information Commissioner's Office suggests children aged 12 or over will often have sufficient maturity and understanding to exercise their own rights. However, there is no fixed age in England, Wales and Northern Ireland, and this should be considered on a case-by-case basis.

Children aged 16 or over will normally be expected to exercise their own right of access. A parent, carer or other person may act on their behalf where the child has clearly authorised them to do so.

Where a parent or carer makes a request on behalf of a child, the School/Trust should consider:

- whether the information is of a type the School/Trust would normally share with the parent or carer, such as attendance, progress, behaviour, school reports, routine correspondence or day-to-day welfare information
- the child's age, maturity and understanding
- the child's wishes and expectations
- whether any authority given by the child is informed and freely given
- whether disclosure would be in the child's best interests
- the nature and sensitivity of the information requested, and
- any relevant safeguarding, confidentiality or court order considerations

Where the child is not sufficiently competent to exercise their own rights, a person with parental responsibility may usually exercise the right on their behalf, unless there is reason to believe that doing so would not be in the child's best interests.

Advice shall be obtained from Plymouth CAST's Data Protection Officer in complex cases.

Preserving relevant information

Once a SAR is received, records potentially falling within the scope should not be deliberately deleted or altered because a request has been made. Where routine deletion is scheduled during the SAR process, the Case Handler should consider whether potentially relevant material needs to be preserved until searches and review have been completed.

Staff must not deliberately:

- delete relevant emails
- amend contemporaneous records
- remove comments or notes
- destroy paper records; or
- otherwise interfere with relevant material

Normal corrections or additions genuinely required for operational purposes may continue, but the original record should be retained where appropriate.

Conducting searches

The School/Trust must undertake reasonable and proportionate searches for personal data within the scope of a SAR. The Case Handler should identify the staff, systems and records most likely to contain the information requested, taking account of the subject matter, relevant time period and how the School/Trust normally records that type of information.

Searches should focus on the systems and records where the requested information would ordinarily be expected to be held, for example safeguarding and behaviour systems, management information systems or personnel records. The School/Trust is not required to search every possible repository simply because personal data might potentially be held there.

Where email or other correspondence is likely to fall within the scope of the request, searches should be appropriately targeted using relevant staff names, date ranges, incidents, subject matters or other suitable search criteria. Where necessary, the requester may be asked for further information to help identify and locate the personal data they are seeking.

Preparing the disclosure

Personal data: When personal data has been located and retrieved, it must be reviewed carefully before disclosure. The requester is only entitled to their own personal data that falls within the scope of the SAR.

Where a document contains both the requester's personal data and other information, for example, internal correspondence about how the School/Trust should manage an incident, apply a procedure or organise its response, the School/Trust may either disclose the document with any necessary redactions applied, or extract the relevant personal data and provide it separately.

Exemptions: A requester is not always entitled to receive all of the information they have asked for. The UK GDPR and Data Protection Act 2018 contain exemptions which may allow or require the School/Trust to withhold certain information.

Depending on the circumstances, this may include information relating to other people, confidential references, legally privileged information, certain safeguarding or health

information, examination information, or information where disclosure could prejudice the prevention or detection of crime.

Where an exemption applies, the relevant information should be removed, redacted or, where appropriate, the requester's personal data may be extracted and provided separately.

Exemptions must be considered carefully and applied only where the legal conditions are met. Advice should be sought from Plymouth CAST's Data Protection Officer where there is any uncertainty.

Disclosure of staff names

Staff names and professional observations should not automatically be redacted from a SAR disclosure. Where the information concerns an education worker, such as a teacher, teaching assistant, SENCO or Headteacher, acting in their professional role, it may be reasonable to disclose their name and relevant professional observations about the data subject, without obtaining their consent.

The School/Trust should still consider the circumstances, including the staff member's role, the nature of the information, whether disclosure would be reasonably expected, and any safeguarding, welfare, confidentiality or security concerns.

Where there is uncertainty, advice should be sought from Plymouth CAST's Data Protection Officer.

Third party consultation

Where records include information provided by, or relating to, an external professional or organisation, the School/Trust should consider whether consultation is appropriate before disclosure. This may include information from the police, social care, health professionals, educational psychologists or other agencies.

Where appropriate, the School/Trust should consult the relevant professional, organisation or their Data Protection Officer about any confidentiality, safeguarding or other concerns that may affect disclosure.

Consultation will not usually be necessary where it is clear that the person making the request has already received the same information, has contributed to the discussions, is aware of the information it contains or where there are no concerns about disclosure.

The final decision on whether to disclose the information rests with the School/Trust. However, the School/Trust will take account of any objections or concerns raised by the third party when deciding whether disclosure is appropriate.

Redactions

Where information needs to be withheld, the relevant sections of the document must be securely redacted before disclosure.

For electronic records, redaction should be carried out using appropriate redaction software, such as Adobe Acrobat Pro or Canva, so that the underlying text is permanently removed and cannot be recovered. Simply highlighting text, changing the font colour or placing a shape over the information is not sufficient.

For paper records, a copy of the original document should normally be used for disclosure. Redactions should be applied to the copy using an appropriate redaction pen or another permanent method that fully obscures the information. The redacted copy should then be checked to ensure that the concealed text cannot be read through, copied, scanned or otherwise reconstructed.

Redactions should be limited to the information that needs to be withheld, while leaving the remaining personal data clear and intelligible. Where extensive redaction would make a document difficult to understand, the School/Trust may instead extract the relevant personal data and provide it separately.

Peer review and SAR disclosure checklist

Before disclosure, the proposed SAR response should be reviewed by a second appropriate member of staff. The reviewer should check that the information falls within the scope of the request, that exemptions and redactions have been applied correctly, and that no information has been included or omitted in error. The Case Handler should review and complete the School/Trust's Subject Access Disclosure Checklist and retain this on file.

Disclosure format

The disclosure should be provided in the format requested by the individual (where reasonable), or otherwise in a format they would reasonably expect to receive. This will usually be by electronic copy or, where requested or appropriate, in paper form.

Disclosure letter and supplementary information

The SAR disclosure should be accompanied by a response letter confirming the outcome of the request and providing any necessary explanation about the information disclosed, withheld or redacted. The School/Trust should use the template SAR response letters when corresponding with the individual making the request.

The individual is also entitled to receive supplementary information about how the School/Trust processes their personal data, including the purposes of the processing, categories of personal data, recipients, retention arrangements and their data protection rights. This information is set out in the School/Trust's Privacy Notice. The SAR response letter templates direct the requester to this information.

Secure disclosure

Personal data must be disclosed using a method appropriate to its sensitivity. Electronic disclosures should normally be sent using a secure method, such as encrypted email, a secure file transfer service or password-protected files, with passwords communicated separately where appropriate. 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, and the School/Trust will comply once written confirmation has been received.

Paper records should be handed directly to the requester, collected by arrangement following appropriate identity checks, or sent using Royal Mail Special Delivery (standard post will not be used for sensitive or confidential information).

Before disclosure, the School/Trust should check the recipient details, attachments and security arrangements to reduce the risk of information being sent to the wrong person.

Retaining a copy and closing the SAR

Once disclosure has been completed, the Case Handler should retain a clear record of how the SAR was handled. This should include:

- a copy of the final response letter
- a copy of the material disclosed to the requester
- the original unredacted material reviewed
- where practicable, a working copy showing or highlighting where redactions were made
- the completed Case Handler SAR Disclosure Checklist, including commentary about decision making and application of exemptions, and
- the date and method of disclosure.

The Chief Operating Officer must be informed when the request has been completed, and will update the Information Request Log to show that the request has been closed.

All SAR records must be stored securely and retained in accordance with Plymouth CAST's retention arrangements.

5. Rectification Requests

Article 16 of the UK GDPR gives individuals the right to have inaccurate personal data corrected and incomplete personal data completed.

Requests can be received in writing including by email, letter or through other communication channels used by the School/Trust, or verbally and should be handled in

accordance with the general requirements set out earlier in this procedure, including identity checks, logging, acknowledgement, timescales, clarification and record keeping.

The School/Trust should identify the information being challenged, consider the individual's reasons and any supporting evidence, and take reasonable steps to determine whether the information is inaccurate or incomplete.

Personal data may be inaccurate where it is incorrect or misleading as a matter of fact. However, an individual's disagreement with a professional opinion, observation, judgement or contemporaneous record does not necessarily mean the information is inaccurate. Where a record accurately reflects what was observed, reported or believed at the time, the School/Trust may retain the original record and, where appropriate, add a supplementary note recording the individual's disagreement or any subsequent clarification.

While the accuracy of disputed information is being considered, the School/Trust should consider whether its use should be temporarily restricted.

Where the School/Trust agrees that information is inaccurate or incomplete, it should correct or complete the record without undue delay. Where the information has previously been shared with another organisation or recipient, the School/Trust should consider whether they also need to be informed of the correction.

Where the School/Trust decides not to make the requested change, the reasons should be documented and explained to the individual in the final response. Where appropriate, the School/Trust should also record that the individual disputes the information.

The outcome should be confirmed using the appropriate template response letter. A copy of the request, relevant evidence, decision-making, any advice obtained and the final response should be retained, and the Information Request Log updated when the request is closed.

6. Erasure Requests

Article 17 of the UK GDPR gives individuals the right, in certain circumstances, to have their personal data erased. This right is not absolute and will not apply where there is a lawful justification for the School/Trust to continue retaining the information.

Requests should be handled in accordance with the general requirements set out earlier in this procedure, including identity checks, logging, acknowledgement, timescales and record keeping.

The School/Trust should identify the personal data the individual would like erased and consider whether the right applies. Erasure may be appropriate where the information is no longer needed, consent has been withdrawn and there is no other lawful basis for

processing, the processing is unlawful, or the individual has successfully objected to the processing.

Information may need to be retained to meet legal, safeguarding, educational, employment, financial or other statutory and operational requirements, or for the establishment, exercise or defence of legal claims. The School/Trust should therefore check the purpose, lawful basis and applicable retention requirements before deleting any information.

Where erasure is agreed, the information should be securely deleted without undue delay and, where appropriate, relevant recipients should be informed. Where the School/Trust decides to retain the information, the reasons should be documented and explained to the individual.

The School/Trust should seek advice from Plymouth CAST's Data Protection Officer where there is any uncertainty about whether the information should be erased or retained.

The request, decision-making, any advice obtained and the final response should be retained, and the Information Request Log updated when the request is closed.

7. Other data protection requests

Article 17 of the UK GDPR gives individuals the right, in certain circumstances, to have their personal data erased. This right is not absolute and will not apply where there is a lawful justification for the School/Trust to continue retaining the information.

Requests should be handled in accordance with the general requirements set out earlier in this procedure, including identity checks, logging, acknowledgement, timescales and record keeping.

The School/Trust should identify the personal data the individual would like erased and consider whether the right applies. Erasure may be appropriate where the information is no longer needed, consent has been withdrawn and there is no other lawful basis for processing, the processing is unlawful, or the individual has successfully objected to the processing.

Information may need to be retained to meet legal, safeguarding, educational, employment, financial or other statutory and operational requirements, or for the establishment, exercise or defence of legal claims. The School/Trust should therefore check the purpose, lawful basis and applicable retention requirements before deleting any information.

Where erasure is agreed, the information should be securely deleted without undue delay and, where appropriate, relevant recipients should be informed. Where the School/Trust

decides to retain the information, the reasons should be documented and explained to the individual.

The School/Trust should seek advice from Plymouth CAST's Data Protection Officer where there is any uncertainty about whether the information should be erased or retained.

The request, decision-making, any advice obtained and the final response should be retained, and the Information Request Log updated when the request is closed.

Appendix A: Summary of Changes

This appendix summarises the key changes made between Versions 5 and 6 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.

Version 6 is a comprehensive, standalone rewrite rather than an incremental update.

1. AI-Assisted Requests (New Section)

- **V5 Policy:** Contained no provisions for requests generated using Artificial Intelligence.
- **V6 Policy:** Introduces explicit rules stating that AI generation does not make a request invalid or automatically excessive. Staff must assess the underlying UK GDPR requirements rather than relying on legal assertions in the AI output, seek clarification if broad, and process repeated AI requests under standard repeated request rules.

2. Statutory "Stop the Clock" Clarification Rules

- **V5 Policy:** Permitted asking for clarification, but the 1-month statutory countdown clock continued to run while waiting for a reply.
- **V6 Policy:** Formally introduces statutory "Stop the Clock" provisions for Subject Access Requests (SARs). The 1-month period pauses on the day clarification is formally requested and resumes on the working day after a satisfactory response is received.

3. Duty to Preserve Records

- **V5 Policy:** Addressed standard searches, but lacked explicit non-deletion instructions upon receipt of a request.
- **V6 Policy:** Introduces a strict duty prohibiting staff from deleting emails, amending contemporaneous notes, destroying paper files, or permitting automated deletion routines to run on records falling within the scope of an active SAR.

4. Standard for Searching Data Repositories

- **V5 Policy:** Required reasonable searches across electronic and paper files without defining search limits.
- **V6 Policy:** Clarifies that searches must be "reasonable and proportionate" and targeted at systems where data is ordinarily held (e.g., MIS, personnel files). Schools are explicitly not required to search every possible repository simply because data might theoretically exist there.

5. Presumption of Non-Redaction for Education Staff

- **V5 Policy:** Stated generally that third-party data could not be disclosed without consent unless reasonable.
- **V6 Policy:** Clarifies that names, roles, and professional observations of education staff (teachers, SENCOs, TAs, Headteachers) acting in their professional capacity should **not** routinely be redacted from SAR disclosures unless specific safety, harassment, or safeguarding risks exist.

6. Rectification Rules: Professional Opinions vs. Factual Errors

- **V5 Policy:** Stated generally that inaccurate data could be corrected.
- **V6 Policy:** Adds an explicit distinction: an individual's disagreement with a professional judgment, observation, or contemporaneous record does **not** render the data "factually inaccurate". In such cases, the original record remains, and a supplementary note recording the disagreement is attached.

7. Document Structure & Layout

- **V5 Policy:** Organized into 11 sections plus Appendix A (Summary of Changes).
- **V6 Policy:** Streamlined into 7 core sections, elevating **Rectification Requests** and **Erase Requests** into standalone, dedicated procedural sections.