Plymouth CAST

Data Protection Request Handling Procedure 2022-24

Approved by:	Plymouth CAST Board
Date:	July 22
Version:	3.0
Review Date:	July 2024

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 Trust'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 Trust's Data Protection Officer Email: dpo@firebirdltd.co.uk

Table of Contents

Data protection rights

The Trust holds personal data about lots of people (data subjects) for example:

- Pupils
- Parents, carers, and siblings
- Employees
- Emergency contacts
- Members, Governors, Trustees and Clerks
- Volunteers
- Visitors to our school
- Job applicants
- Temporary workers and agency staff
- People who make a complaint, information request or enquiry

Data subjects have several rights under the data protection legislation (the UK GDPR and the Data Protection Act 2018). In summary, people have the right to:

- Be kept informed about the use, sharing and storage of their data (this is a privacy notice)
- Request access to their personal data held by the Trust (this is a subject access request)
- Have inaccurate or incomplete data about them 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.

Data protection requests

Data subjects who want to exercise their rights should make a 'data protection request' and send this to admin@plymouthcast.org.uk Edmund Rice Building, St Boniface College, Boniface Lane, Manadon Park, Plymouth, PL5 2AG. Data subjects can make their request in writing or verbally. If a verbal request is received (e.g. during a telephone call or in person), Rose Colpus-Fricker will write to the individual summarising what was requested and will ask them to confirm their understanding is correct. Where required, the Trust shall make reasonable adjustments for individuals who want to make a request, in line with their duties under the Equality Act 2010.

The most common request received by the Trust is a 'Subject Access Request' (a SAR). This is when the requester wants a copy of their personal data. However, other types of data protection requests may also be received, such as a formal request to update, amend or delete records or a request to stop receiving fundraising information or other forms of direct marketing from the school.

Requests do not have to mention 'data protection' or the 'GDPR;' it is therefore important that correspondence which does not mention these phrases, are not inadvertently overlooked.

Logging and acknowledgment

Upon receipt of a data protection request, the Trust's Data Protection Link Officer will record the request on the Information Request Log. An acknowledgement will be sent using the Trust's template letters. If the Trust is not satisfied with the requester's identity, it will seek further confirmation. In such cases, the Trust may ask the requester to provide a copy of their official identification, such as a passport, driving licence or utility bill.

If a request is made on behalf of a data subject (e.g. by a solicitor or spouse), the requester must provide evidence of their entitlement to receive the response. This may be demonstrated by providing written consent from the data subject; a document showing they have power of attorney (this will be relevant where the data subject does not have the mental capacity to make the request themselves); or a court order. Advice shall be sought from the Data Protection Officer if there is doubt regarding a requester's entitlement to receive the response.

Timescales and fees

The Trust must respond to requests as soon as possible and in any case within one calendar month. If this is not possible because the following month is shorter, the date for response (the deadline) will be the last day of that month. If the deadline falls on a weekend or a public holiday, the Trust shall respond the next working day.

The countdown starts the day the request is received, unless evidence of entitlement or clarification is required, in which case it starts when this further information is received. The Trust can extend the time to respond by a further two months, if the request is complex or it has received a number of requests from the individual. In such a case, the Trust shall inform the individual within one month of receiving their request and explain why the extension is necessary.

The Trust cannot charge a fee for responding to a data protection request unless the Trust considers the request to be 'manifestly unfounded or excessive.' In such cases, the Trust can either refuse the request entirely or comply with it but charge a 'reasonable fee' for the administrative costs of doing so.

'Manifestly unfounded or excessive' has a wide meaning, but a request may fall into this category if:

- it is malicious and is being used to harass the Trust and has no real purpose other than to cause disruption
- the requester makes unsubstantiated accusations against the Trust or specific employees
- the requester is targeting a particular employee who they have a personal grudge with
- the requester systematically sends different requests to the Trust as part of a campaign, with the intention of causing disruption
- the request repeats the substance of previous requests, and a reasonable interval has not elapsed
- the request overlaps with other requests

This list is not exhaustive.

The Trust can also charge a reasonable fee for the administrative costs of complying with a request if the individual asks for further copies of their data following a request. If the Trust decides to charge a fee, it shall contact the individual promptly and inform them. The Trust is not required to comply with the request until it has received payment.

Actioning the request

The DPO shall make enquiries with relevant employees and governors / members and trustees (as appropriate) about the request. If the Trust does not believe it is required to action the particular request because, for example, it does not hold the information or if the Trust's interests override the individual's, it shall confirm this position clearly and in writing, within one month. The Trust shall discuss and seek advice about refusals of this nature with the Data Protection Officer, before issuing the response.

Subject access requests (SARs)

Requests from pupils

A pupil can request a copy of their personal data (i.e. make a SAR), if they have sufficient maturity to do this, for example, they understand their rights; they know what it means to make a request and can understand the information they are given. The Information Commissioner's Office suggests that it may be reasonable in most cases, to assume a child who is aged 12 years or over has sufficient maturity to be able to make a request, unless the contrary is shown.

A pupil that does not have sufficient maturity, should have a parent/carer make this request on their behalf. This also applies if it would not be in the child's best interests to release the records to them directly, for example, if the information could cause them significant distress.

Requests from parents

A parent/carer who has parental responsibility can request a copy of their child's personal data if:

- it is routine school information that they would usually receive as a parent or
- their child authorises this (if they have sufficient maturity) or
- it is clearly in their child's best interests

When assessing this, the Trust will consider the following:

- The child's level of maturity and their ability to make decisions
- The nature of the data being requested
- Any duty of confidentiality owed to the child
- Consequences of allowing access
- Detriment to the child if their parent cannot get access
- Views of the child as to whether their parent should have access
- Any court orders or restrictions relating to parental access or responsibility

The 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 Trust shall consider the validity of any consent received from a child (under 18 years old); consent is only valid if the child is fully informed and understands what they are consenting to, and it is freely given (i.e. not through coercion).

Gathering the information requested

Upon receipt of a SAR, the DPO shall identify whether the Trust holds the information being requested, and if so, where it is stored. This will involve searching the Trust's electronic and paper systems and may require contacting relevant Trust employees or governors who are likely to hold the personal data. Data subjects are entitled to receive their data stored in any format, whether it is on paper or electronically held. Draft documents, safeguarding observations and emails are all potentially disclosable (unless an exemption applies).

All employees and governors shall provide their full co-operation when a SAR is received. All information requested must be given to the DPO, so they can decide (alongside the Data Protection Officer and the Headteacher as necessary) what is and is not disclosable under the data protection legislation. Concerns about the release of information should be shared with the DPO, so they can consider and where appropriate apply an 'exemption' to withhold that information.

Exemptions

The data protection legislation provides several exemptions which permit the Trust to withhold certain information from data subjects. The following is a summary of some of the exemptions:

The Trust does not have to release information if:

- the information contains personal data about another person and the Trust does not have their consent to release that information, or it is not reasonable to disclose it without their consent
- disclosure is likely to cause someone serious harm to their mental or physical health
- disclosure would prejudice crime prevention or detection, prosecution of an offender or the assessment or collection of tax or other duties
- the information contains confidential communications between the Trust and its legal advisors
- it is for a reference which has been provided in confidence
- it is for education data given to a court as part of court proceedings
- another law prohibits disclosure
- it contains management forecasting or management planning and disclosure at that time, could prejudice the effective running of the Trust
- disclosure is likely to prejudice negotiations with the data subject

This list is not exhaustive

Preparing the disclosure

If an exemption applies, the relevant text will be redacted (i.e. obscured from view). This may be applied using redaction software or blacking out the relevant text with a marker pen on paper copies. If a document is redacted using a marker pen, the requester shall be given a photocopy of this document and not the original penned version, to ensure the redacted text does not show through the ink.

If the file contains correspondence or documentation provided by an external professional, (for example a police officer, health practitioner or social worker), the author shall be consulted prior to the release of the information (where available, the professional's Data Protection Officer will be contacted in the first instance to facilitate the consultation), except where the document or email clearly shows that the requester was copied into the email or was sent that document, in which case it may be released without consultation.

Disclosing the information

When the disclosure is ready, then content shall be checked by another colleague (where possible), to ensure it meets the scope of the request and all exempt information has been redacted.

The DPO shall complete the 'Subject Access Request Disclosure Checklist' and save this along with a copy (electronic or a paper copy) of the disclosure and close the request on the Information Request Log. Where documents have been redacted, the unredacted version shall also be held within a separate part of the file in case of subsequent complaint by the requester. This is to enable the complaint handler ease of access to any disputed documents.

Disclosures shall be made in the format requested (or expected) by the requester. Usually this means being given a physical copy or being emailed the disclosure. Disclosures made by

email shall be sent securely using Egress Switch, unless the requester specifically requests that the information is sent to them using unencrypted email. In such cases, the applicant shall be informed that the Trust does not recommend this form of transfer, as it cannot guarantee the security of the information. If the requester insists that it be provided this way, the Trust shall follow their instruction upon confirmation of this in writing.

If the requester is to receive a physical copy, this can be:

- delivered by hand, or
- collected from the Trust, or
- posted using Royal Mail Special Delivery (standard mail should not be used to send sensitive or confidential information)

Complaints

If a requester is not satisfied with the Trust's response to their Data Protection Request, they should in the first instance write to the person who responded to the request, expressing their dissatisfaction and the reasons why, or contact the Data Protection Officer directly at DPO@firebirdltd.co.uk.

If the matter is not able to be addressed informally, the requester should follow the Trust's formal complaints procedure
https://www.plymouthcast.org.uk/web/other_policies__key_information/485001

If a requester remains dissatisfied with the outcome of their complaint, they can escalate this to the Information Commissioner's Office by writing to: Customer Contact, Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow SK9 5AF or email: casework@ico.org.uk