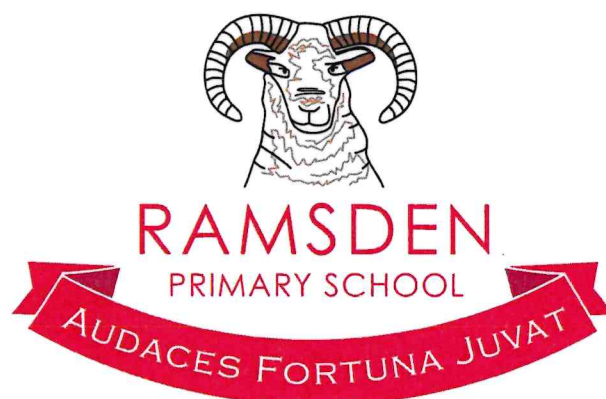


RAMSDEN PRIMARY SCHOOL



SUBJECT ACCESS REQUEST POLICY

UK GDPR and Data Protection Act 2018

Compiled by	Headteacher	September 2026
Approved By	Chair of Governors September 2026	Headteacher  September 2026
To be reviewed		Autumn Term 2026

Contents

1. Introduction
2. Receiving a Subject Access Request
3. What is a Subject Access Request?
4. Requirements for a Valid Request
5. Time Limit for Responding to a Request
6. Information to be Provided in Response to a Request
7. How to Locate Information
8. Information to be Supplied in Response to a Request
9. Disclosing Personal Data Relating to Third Parties
10. How the Information Should be Provided
11. Requests Made by Third Parties on Behalf of an Individual
12. Exemptions to the Right of Subject Access
13. Deleting Personal Data in the Normal Course of Business
14. Consequences of Failing to Comply with a Request
15. Roles and Responsibilities

1. Introduction

1.1 Ramsden Primary School holds personal data about a range of individuals, including pupils, parents and carers, employees, job applicants, governors, suppliers, contractors, professional contacts and other individuals who interact with the school.

1.2 Under the UK GDPR and Data Protection Act 2018, individuals (known as 'data subjects') have a general right to request access to personal data that the school holds or processes about them, subject to certain conditions and exemptions. These requests are known as Subject Access Requests (SARs).

1.3 The DPO is responsible for ensuring that Subject Access Requests are handled in accordance with applicable data protection requirements and that staff understand their responsibilities when a request is received.

1.4 This policy provides guidance to Ramsden Primary School staff on how Subject Access Requests should be handled. It is primarily an internal operational policy and should not be treated as the school's privacy notice.

1.5 The policy is aimed particularly at staff who are authorised to handle Subject Access Requests. For all other staff, it explains what to do if a request is received and how to recognise a potential Subject Access Request.

1.6 Failure to comply with data protection requirements can place both the school and individuals at risk. Failure by staff to comply with this policy may be addressed through the school's appropriate management or disciplinary procedures.

1.7 Questions about Subject Access Requests should be referred promptly to the DPO or the person designated by the school to coordinate data protection matters.

2. Receiving a Subject Access Request

2.1 If a member of staff receives a request for access to personal information and is not authorised to handle Subject Access Requests, they must pass it promptly to the Headteacher or designated data protection lead, who will refer it to the DPO as appropriate.

2.2 Staff should not delay forwarding a request because they are uncertain whether it constitutes a Subject Access Request. If in doubt, it should be referred for advice.

2.3 A request may be received by email, letter, verbally, through an online communication system or by another means. A request does not have to use the words 'Subject Access Request' or refer specifically to the UK GDPR.

2.4 Staff who receive a potential Subject Access Request must not delete, alter, conceal or otherwise interfere with relevant personal data because a request has been made.

2.5 Staff must not respond substantively to a Subject Access Request unless authorised to do so.

3. What is a Subject Access Request?

3.1 A Subject Access Request is a request from an individual for access to personal data that Ramsden Primary School processes about them.

3.2 For example, a request such as 'please provide me with a copy of all the information you hold about me' may constitute a Subject Access Request even if it does not expressly refer to personal data or the UK GDPR.

3.3 Requests may relate to specific records or to a wider range of information. The school should establish the scope of the request where necessary, but should not impose unnecessary barriers on the exercise of the right of access.

4. Requirements for a Valid Request

4.1 A Subject Access Request does not normally have to be made using a particular form. Requests may be made verbally or in writing.

4.2 The school must be satisfied as to the identity of the person making the request where this is necessary and proportionate. The school may request reasonable evidence of identity where there is a genuine need to verify identity.

4.3 The school may ask the requester for information that will help locate the relevant data where the request is not sufficiently clear. For CCTV requests, this may include a photograph or description of the person, together with the date, approximate time and location of the recording where available.

4.4 Requests are generally free of charge. A reasonable fee may be charged, or a request may be refused, where legislation permits this because a request is manifestly unfounded or excessive, including where requests are repetitive.

4.5 If additional information is genuinely required to identify the requester or locate the information, the DPO will contact the requester promptly and explain what is required.

5. Time Limit for Responding to a Request

5.1 The school will normally respond to a valid Subject Access Request without undue delay and, in any event, within one month of receipt.

5.2 Where a request is complex or where the individual has made a number of requests, the school may extend the response period by up to a further two months where permitted by law.

5.3 If an extension is required, the school will inform the requester within the initial one-month period and explain why additional time is necessary.

5.4 The DPO will oversee the response timetable and ensure that appropriate records are maintained.

6. Information to be Provided in Response to a Request

6.1 Subject to applicable conditions and exemptions, an individual is entitled to access their personal data and information about its processing, including, as applicable:

6.1.1 the personal data processed about them;

6.1.2 the purposes for which the data are processed;

6.1.3 the categories of personal data concerned;

6.1.4 recipients or categories of recipients to whom the personal data have been or may be disclosed;

6.1.5 information about the source of the personal data where the school did not obtain it directly from the individual;

6.1.6 the envisaged retention period, or the criteria used to determine it; and

6.1.7 information about relevant automated decision-making or profiling where applicable.

6.2 The information supplied should be understandable and presented in an accessible form. Technical terms, abbreviations and codes should be explained where necessary.

6.3 Where an automated decision has been made about an individual and the relevant statutory requirements apply, the school will provide the information required by data protection law.

7. How to Locate Information

7.1 Personal data may be held across a number of electronic and manual systems. The type and scope of information requested should be established at the outset so that appropriate searches can be carried out.

7.2 Depending on the nature of the request, relevant sources may include:

7.2.1 school information management systems and pupil records;

7.2.2 email accounts and relevant electronic communications;

7.2.3 networked and non-networked computers and servers;

7.2.4 HR and personnel records;

7.2.5 safeguarding and pastoral records, where applicable;

7.2.6 CCTV recordings, where the request concerns images of the requester;

7.2.7 paper files and other manual records;

7.2.8 information held by relevant data processors acting on the school's behalf; and

7.2.9 other systems identified as relevant by the DPO.

7.3 Searches should use appropriate identifiers, such as the individual's name, pupil number, employee number or other relevant identifier.

7.4 Staff must take reasonable care to ensure that searches are sufficiently thorough for the scope of the request and must keep the DPO informed of any difficulty locating information.

8. Information to be Supplied in Response to a Request

8.1 Following the search, the DPO will determine which information constitutes the requester's personal data and should therefore be supplied, subject to applicable exemptions and the rights of other individuals.

8.2 Personal data includes information relating to an identified or identifiable individual. Information relating solely to companies or other legal entities is not personal data, although information relating to individuals within organisations may be.

8.3 The right of access is subject to conditions and exemptions, particularly where disclosure would reveal personal data relating to another individual.

8.4 Where appropriate, the school may provide copies of existing documents containing the individual's personal data, subject to redaction and any applicable exemptions.

8.5 Where the information includes CCTV images, the school will provide images in a format that enables them to be viewed clearly, subject to appropriate redaction or other measures required to protect the rights and freedoms of other individuals.

9. Disclosing Personal Data Relating to Third Parties

9.1 If the requested personal data also identifies another individual, the DPO will consider whether disclosure would reveal that person's personal data and whether the request can be complied with without disclosing information about the third party.

9.2 Where possible, the school will redact or otherwise remove third-party personal data while providing the requester's own personal data.

9.3 If third-party information cannot reasonably be separated from the requester's information, the DPO will consider whether disclosure is reasonable in all the circumstances. This may include considering any duty of confidentiality, the expectations of the third party, whether consent is appropriate, the nature of the information and the importance of the information to the requester.

9.4 Consent from a third party is not automatically required before disclosure. The question is whether it is reasonable to disclose the information in the circumstances, taking account of the applicable legal requirements.

9.5 Each request will be considered on its individual facts.

9.6 CCTV requests require particular care where other identifiable individuals appear in the footage. The school will consider whether blurring or other measures are necessary to avoid an unfair intrusion into another person's privacy or unwarranted harm or distress.

9.7 The school will keep a record of significant decisions concerning third-party information, including the reasons for the decision.

10. How the Information Should be Provided

10.1 The individual is entitled to receive a copy of their personal data, subject to applicable exemptions and restrictions.

10.2 The school will normally provide information in a secure digital form where appropriate, unless another format is requested or a different format is more suitable.

10.3 Information must be securely transmitted and appropriate safeguards must be used where sensitive or confidential information is being provided.

10.4 CCTV images and other visual material should be provided in a form that allows them to be viewed clearly, with appropriate redaction where required.

11. Requests Made by Third Parties on Behalf of an Individual

11.1 A Subject Access Request may sometimes be made by a third party acting on behalf of an individual. Examples may include parents or carers, legal representatives, solicitors, people acting under a power of attorney or another person with appropriate authority.

11.2 The school must establish that the third party is authorised to act on behalf of the individual before providing personal data, unless another lawful basis or legal requirement applies.

11.3 Requests concerning children require particular care. The DPO will consider the child's age, understanding, circumstances, the nature of the information and the relevant legal requirements when determining how the request should be handled.

11.4 The DPO will assess requests made by third parties and will determine what information, if any, can be disclosed.

12. Exemptions to the Right of Subject Access

12.1 In certain circumstances, legislation provides exemptions or restrictions to the right of subject access. These must be considered on a case-by-case basis and only to the extent permitted by law.

12.2 Crime detection and prevention: information may be withheld where the relevant statutory conditions are met and disclosure would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

12.3 Confidential references: certain confidential references given or received for employment, education, training, appointment to office or provision of services may be exempt from disclosure where the statutory conditions apply.

12.4 Legal professional privilege: personal data contained within legally privileged material may be exempt from disclosure.

12.5 Management information: certain personal data relating to management forecasting or planning may be exempt where the statutory conditions apply.

12.6 Negotiations: certain personal data consisting of records of the school's intentions in relation to negotiations with the individual may be exempt where disclosure would be likely to prejudice those negotiations.

12.7 Other statutory exemptions may apply depending on the nature and circumstances of the request. Staff must not decide to withhold information without consulting the DPO.

13. Deleting Personal Data in the Normal Course of Business

13.1 The school must not alter, delete, conceal or destroy personal data simply because an individual has made a Subject Access Request.

13.2 Normal and lawful housekeeping, retention and deletion processes may continue where the amendment or deletion would have occurred regardless of the Subject Access Request.

13.3 Staff must not amend or delete information in order to avoid supplying it in response to a Subject Access Request.

13.4 Where information relevant to a request is subject to a routine deletion process, the DPO should be informed so that the position can be considered appropriately.

14. Consequences of Failing to Comply with a Request

14.1 Failure to comply with applicable Subject Access Request requirements may result in a complaint to the Information Commissioner's Office (ICO), regulatory action or other legal consequences.

14.2 An individual may, where the relevant legal conditions are met, seek compensation for damage or distress caused by a breach of data protection law.

14.3 A court or other competent authority may require the school to comply with its data protection obligations.

14.4 Staff are therefore expected to treat Subject Access Requests promptly, carefully and confidentially.

15. Roles and Responsibilities

Role	Key responsibility
Headteacher	Ensure the school has effective arrangements for responding to Subject Access Requests and that staff understand their responsibilities.
DPO / Data Protection Lead	Oversee SARs, advise on scope and exemptions, coordinate searches and disclosures, maintain appropriate records and provide data protection advice.
Senior Leadership Team / authorised staff	Ensure requests are referred promptly, support appropriate searches and do not disclose information without authorisation.
All staff	Recognise potential SARs, forward them promptly, preserve relevant information and maintain confidentiality.
Data processors / external providers	Assist the school with searches or information retrieval where required under contractual and data protection arrangements.

Document control: This policy should be read alongside Ramsden Primary School's Data Protection Policy, Privacy Notices, CCTV Policy, Data Breach Procedure, Records Retention arrangements and Complaints Policy.