



EMMAUS

CATHOLIC MAC

Dealing with Requests for Personal Information Policy

Version	1.0
Date created/updated	03.08.23
Ratified by	Compliance / Full Board
Date ratified	10.09.23
Date issued	12.09.23
Policy review date	01.09.25
Post holder responsible	Chief Finance and Operations Officer

Commitment to Equality:

We are committed to providing a positive working environment which is free from prejudice and unlawful discrimination and any form of harassment, bullying or victimisation. We have developed a number of key policies to ensure that the principles of Catholic Social Teaching in relation to human dignity and dignity in work become embedded into every aspect of school life and these policies are reviewed regularly in this regard.

This Dealing with Requests for Personal Information Policy has been approved and adopted by Emmaus Catholic Multi Academy Company on 10th September 2023 and will be reviewed in September 2025.

Signed by Director of Emmaus Catholic MAC:

Signed by CSEL for Central Team:

Schools to which this policy relates:

Signed by Principal for – Hagley Catholic High School

Signed by Principal for – Our Lady of Fatima Catholic Primary School:

Signed by Principal for – Our Lady & St Hubert’s Catholic Primary School:

Signed by Principal for – St Ambrose Catholic Primary School:

Signed by Principal for – St Francis Xavier Catholic Primary School:

Signed by Principal for – St Gregory’s Catholic Primary School:

Signed by Principal for – St Joseph’s Catholic Primary School

Signed by Principal for – St Mary’s Catholic Primary School:

Signed by Principal for – St Philip’s Catholic Primary School:

Signed by Principal for – St Wulstan’s Catholic Primary School:

Contents

1	Aims	4
2	Legislation and Guidance	4
3	Requests for Personal Information	4
4	Roles and Responsibilities	6
5	When Can Individuals Exercise Their Right of Access	7
6	Requests About Pupils	7
7	What to Consider When Responding to a Request	7
8	Requesting ID	8
9	Charging for a Request	8
10	How to Find and Retrieve the Relevant Information	9
11	Can we Refuse to Comply with a Request	10
12	Information About Other People Including Witness Statements	10
13	Confidential References	11
14	Complying with Requests During Grievance Process or Tribunal	11
15	Disclosing Routine Emails that Refer to Pupils or Staff	12
16	Searching Across Social Media Accounts	13
17	CCTV Footage Request – what to disclose	13
18	Can the Right of Access be Enforced	13
19	What to do if Individual is not Happy with SAR Response	13
20	Response Time	14
21	Retention	14

Appendix 1 – Data Protection Checklist

DEFINITIONS

The Company's standard set of definitions is contained at [Definition of Terms](#) – please refer to this for the latest definitions.

1. Aims

- 1.1 Emmaus Catholic Multi Academy Company (“the MAC”) aims to ensure that all personal data collected about staff, pupils, parents, directors, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.
- 1.2 This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and Guidance

- 2.1 This policy meets the requirements of the:
 - UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
 - Data Protection Act 2018 (DPA 2018)
 - Equality Act 2010
- 2.2 It is based on guidance published by the Information Commissioner’s Office (ICO) on the GDPR.
- 2.3 The SEN Team will be required to process the request under Regulation 17 of the Special Educational Needs and Disability Regulations 2014 (S.I. 2014/1530) and not under Data Protection rules.

3. Requests for Personal Information

- 3.1 Schools will often receive requests from pupils, parents or staff asking for all personal information that is held by the school.
- 3.2 Parent, Guardian or teacher/staff information held at the school can be accessed as follows:
 - Non pupils can request their own personal information by submitting a Data Subject Access Request (DSAR) in line with Data Protection Law. Data Subjects are only entitled to their own personal data and not anyone else’s.
- 3.3 Pupil information held at school can be accessed as follows:

- Pupils can request their own personal information by submitting a Data Subject Access Request (DSAR) in line with Data Protection Law. Parents or someone with parental responsibility are only entitled to personal information that the school holds about their child if the pupil has provided their consent or if the child is unable to act upon their own behalf. This is normally where the child is under 12 years of age.
- A parent has the right to access the child’s educational record in accordance with The Education (Pupil Information) (England) Regulations 2005. This includes a formal record of the pupil’s academic achievements, other skills, talents and educational progress (defined in Schedule 3, Part 4 of the Data Protection Act 2018).

3.4 Parental Responsibility must be confirmed before the release of any information.

3.5 Below are some examples of the information that would fall within each category.

<u>Educational Record</u>	<u>Personal Information</u>
Assessment information and academic achievements including school reports.	Information provided by another parent or by other pupils in the school
Attendance information	Accident Report
Pupil contact information	CCTV Footage – Please see additional note below.
Personal Education Plan	
Education and Health Care Plan*	
Behaviour and incident monitoring reports including staff statements, fact finding information	

4. Roles and Responsibilities

4.1 Governing body (Directors and LGB)

The Directors have overall responsibility for ensuring that the MAC complies with all relevant data protection obligations.

The Local Governing Bodies (“LGB”) have responsibility for ensuring that the school’s comply with all relevant data protection obligations.

4.2 Data protection officer

The Senior Information Risk Owner (SIRO), Chief Finance and Operations Officer, is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the directors and, where relevant, report to the board their advice and recommendations on MAC data protection issues.

The SIRO is also the first point of contact for individuals whose data the MAC processes, and for the ICO.

Full details of the SIRO’s responsibilities are set out in their job description.

Our MAC SIRO is Amanda Hodder, Chief Finance and Operations Officer and is contactable via ahodder@emmausmac.com

Each school within Emmaus Catholic Multi Academy Company will appoint an Information Asset Owner (IAO) to act as the data protection advisor on site. All Data Protection queries are to be discussed in schools with the Information Asset Owner (IAO), who must then report to the DPO / SIRO for guidance.

Emmaus Catholic Multi Academy Company procure the services of an External DPO working on behalf of the MAC. They can answer any questions you have about what the MAC does with your information. If you or your parents/guardian want to speak to them, then you can do at:

YourIG Data Protection Officer Service
Dudley MBC
The Council House
Dudley
West Midlands
DY1 1HF

Email: YourIGDPOService@dudley.gov.uk

5. When Can Individuals Exercise their Right of Access

- 5.1 An individual can make a SAR verbally or in writing, including on social media. A request is valid if it is clear that the individual is asking for their own personal data.
- 5.2 An individual does not need to use a specific form of words, refer to legislation or direct the request to a specific contact. If the individual is asking for any information held about them or their child/children, we will treat this as a SAR and respond accordingly.
- 5.3 An individual may ask a third party (e.g., a relative, friend or solicitor) to make a SAR on their behalf. Before responding, the MAC need to be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of their authority.
- 5.4 Once the evidence is received by the MAC it needs to be satisfied that the third party is acting on behalf of the data subject before complying with the request.

6. Requests about Pupils

- 6.1 Before responding to a SAR for information held about a child, the MAC should consider whether the child is mature enough to understand their rights. If the request is from a child and the MAC is confident, they can understand their rights, the MAC should usually respond directly to the child. The MAC may, however, allow the parent or guardian to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.
- 6.2 If a child is competent, they may authorise someone else, other than a parent or guardian, to make a SAR on their behalf.

7. What to Consider When Responding to a Request.

- 7.1 The MAC must comply with a SAR without undue delay and at the latest within one month of receiving the request. The school can extend the time to respond by a further two months if the request is complex or the school have received a number of requests from the individual, e.g., other types of requests relating to individuals' rights.
- 7.2 If the school process a large amount of information about an individual, the school may be able to ask them to specify the information or processing activities

their request relates to, if it is not clear. The time limit for responding to the request is paused until the school receive clarification, although it should supply any of the supplementary information it can do within one month.

- 7.3 The 1 month’s response deadline for SARs includes any school holidays. The clock does not stop for the holidays therefore the office@ email accounts should be monitored periodically throughout the holiday by the principal.

8. Requesting ID

- 8.1 The MAC must be satisfied that they know the identity of the requester (or the person the request is made on behalf of). If the MAC are unsure, they can ask for information to verify an individual’s identity. The timescale for responding to a SAR does not begin until the school have received the requested information. However, the MAC should request ID documents promptly.

9. Charging for a Request

- 9.1 In most cases the school cannot charge a fee to comply with a SAR.
- 9.2 However, it can charge a ‘reasonable fee’ for the administrative costs of complying with a request if it is manifestly unfounded or excessive, or if an individual requests further copies of their data.
- 9.3 Any requests for personal information, other than the educational record, should be dealt with in line with the Data Protection Act. A fee can only be charged where the request is manifestly unfounded or excessive. You can also charge a fee if an individual requests further copies of their information following a request. If a fee is going to be charged, the requestor will need to be informed of this at the outset. You do not need to comply with the request until you have received the fee.
- 9.4 Educational Records are charged on the number of pages that are provided; however, the parents can come and view the information free of charge at the school. The charges for educational records are set out below.

<u>Number of Pages</u>	<u>Maximum Fee</u>
1-19	£1.00
20-29	£2.00
30-39	£3.00
40-49	£4.00
50-59	£5.00
60-69	£6.00

70-79	£7.00
80-89	£8.00
90-99	£9.00
100-149	£10.00
150-199	£15.00
200-249	£20.00
250-299	£25.00
300-349	£30.00
350-399	£35.00
400-449	£40.00
450-499	£45.00
500+	£50.00

10. How to Find and Retrieve the Relevant Information

- 10.1 An individual is entitled to a copy of their personal data and to other supplementary information (which largely corresponds with the information that the MAC provides in the privacy notice). If an individual makes a request electronically, the MAC should provide the information in a commonly used electronic format, unless the individual requests otherwise.
- 10.2 When deciding what format to use, the MAC should consider both the circumstances of the particular request and whether the individual has the ability to access the data the MAC provide in that format.
- 10.3 It is good practice to establish the individual's preferred format prior to fulfilling their request. Alternatives can also include allowing the individual to access their data remotely and download a copy in an appropriate format.
- 10.4 If an individual asks, the MAC can provide a verbal response to their SAR, provided that the MAC have confirmed their identity by other means. The MAC should keep a record of the date they made the request, the date the MAC responded, details of who provided the information and what information the MAC provided.
- 10.5 When searching for data in emails and files it is not sufficient to only search for the name of the individual. You must also search for the initials and search any known dates and look for records where the individual can be identified even if not named.

10.6 As the data controller of the information the MAC is responsible for taking all reasonable steps to ensure compliance.

11. Can We Refuse to Comply with a Request

11.1 Where an exemption applies, the MAC may refuse to provide all or some of the requested information, depending on the circumstances. The MAC can also refuse to comply with a SAR if it is manifestly unfounded or manifestly excessive.

11.2 If the MAC refuses to comply with a request, it must inform the individual of: the reasons why; their right to make a complaint to the ICO; and their ability to seek to enforce this right through the courts.

11.3 Whilst there is no requirement to quote the exemption to the requestor, you should explain your reasons for the refusal in plain English so that the requestor can clearly understand. The ICO will want to know the exemption used to refuse the request if contacted therefore it is best practice to quote the exemption to the individual for clarity.

12. Information About Other People Including Witness Statements

12.1 Personal information can cover more than one person. Therefore, responding to a SAR may involve providing information that is about both the requester and someone else.

12.2 The UK Data Protection Act 2018 says the MAC do not have to comply with a SAR if doing so means disclosing information which identifies someone else, except where:

- they consent to the disclosure; or
- it is reasonable to comply with the request without that person's consent.
- To determine whether it is reasonable to comply without consent, the MAC must consider all the relevant circumstances, including:
 - the type of information that would be disclosed.
 - any duty of confidentiality the MAC owe to the other person/people.
 - any steps the MAC took to try to get the other person's consent.
 - whether the other person is capable of giving consent; and
 - any stated refusal of consent by the other person.

12.3 The MAC must respond to the requester whether or not it decides to disclose information about a third party. The MAC must be able to justify its decision to disclose or withhold information about a third party, so it should keep a record of what the MAC decides to disclose or not and why.

13. Confidential References

13.1 The MAC may receive a SAR from a member of staff for references. These could cover references that the MAC either provided to other organisations or that the MAC has received. However, under UK GDPR, confidential references are exempt, when provided for the purposes of:

- education, training, or employment of someone.
- someone working as a volunteer.
- appointing someone to office; or
- provision of any service by someone.

13.2 The exemption applies regardless of whether the MAC give or receive the reference. It is important to note that this only applies to references that the MAC give in confidence. The MAC should make it clear to staff and those providing references whether the MAC treat them as confidential. This can be noted in the privacy notice (Workforce and Recruitment), staff handbook or MAC policies.

13.3 However, if it is unclear whether the MAC are treating references as confidential, it should consider requests on a case-by-case basis, taking into account the following:

- any clearly stated assurance of confidentiality that the MAC has given to the referee.
- any reasons the referee may give for withholding consent.
- the likely impact of the reference on the requester.
- any risk that disclosure may pose to the referee; and
- the requester's interest in being able to satisfy the accuracy and truthfulness of the reference.

14. Does The School Need to Comply If the Member of Staff Is Going Through a Tribunal or Grievance Process

14.1 Yes. People have the right to obtain a copy of their personal information from the MAC. The MAC cannot simply refuse to comply because the member of staff is undergoing a grievance or tribunal process, and the MAC believe they intend to use their personal information to obtain information for potential litigation.

14.2 If the MAC believe it isn't appropriate to disclose the relevant information, it must demonstrate what exemption it is using and why. It is important to note that

whilst there may be separate rules for disclosing information in the course of a tribunal, the MAC must comply with a SAR. This applies even if there may be some cross-over in the information supplied.

- 14.3 However, even if the MAC have already disclosed the information through another statutory process, such as in employment tribunal proceedings, this does not mean that the MAC can refuse to comply with a SAR.
- 14.4 The MAC should bear in mind that the information disclosed during the tribunal proceedings is given to the member of staff's legal representative and not to the member of staff. The MAC cannot assume that the member of staff can access any or all the information, just because the MAC have provided it to their solicitor.
- 14.5 They may also have changed their legal representative during the case. Carefully consider the circumstances of the request and ensure the MAC provides all the member of staff's personal information that they're entitled to.
- 14.6 In the event of an employee requesting personal information during a grievance process or if the principal is concerned the request could be litigious the principal must contact the SIRO (CFOO) and the MAC solicitors for support.

15. Does The MAC Need to Disclose Routine E-Mails Which Refers to Pupils or a Member of Staff

- 15.1 The right of access only entitles the requestor to obtain a copy of their personal information from the MAC. The MAC should consider what information in the e-mail is the personal information of the requester. It also depends on the contents of the e-mail and the context of the information it contains.
- 15.2 Ultimately, it is for the MAC to determine whether any of the information in the e-mail is the requester's personal information. However, it is important to remember:
 - the right of access only applies to the requester's personal information contained in the e-mail. This means the school may need to disclose some or all of the e-mail to comply with the SAR.
 - just because the contents of the e-mail are about a business matter, this does not mean that it is not the requester's personal information. This depends on the content of the e-mail and whether it is about the requester; and
 - just because the requester receives the e-mail, this does not mean that the whole content of the email is their personal information. Again, the context of the information is key to deciding this.

16. Would The MAC Have to Search Across Any Social Media Accounts

- 16.1 If the MAC uses social media platforms such as Facebook, WhatsApp, Twitter and chat channels on Microsoft Teams for school purposes, then as data controller for the information processed on those pages this would also need to be searched.
- 16.2 Therefore, if the MAC receive a SAR, it must search these platforms for any personal information if it falls within scope.

17. We've Had a Request for CCTV Footage, But It Contains Images of Other People. Do We Have to Disclose It

- 17.1 Yes. Individuals who request footage that contains personal information relating to themselves, have a right to receive that information under data protection legislation. When installing CCTV, the MAC should make sure it chooses a system that allows it to easily locate and extract personal information in response to subject access request.
- 17.2 The MAC should also ensure it allows for the redaction of third-party information, where this is necessary. If the MAC CCTV system has this functionality, it will likely enable it to comply with its data protection obligations.
- 17.3 However, if the MAC CCTV system does not have this functionality, it will still need to endeavour to comply with its obligations. However, the MAC should only disclose the footage if it has the other people's consent to do so, or if it's reasonable to do so without their consent.

18. Can The Right of Access Be Enforced

- 18.1 Yes. In appropriate cases, the ICO may take action against a data controller or data processor if they fail to comply with data protection legislation. The ICO will exercise these enforcement powers in accordance with their Regulatory Action Policy.
- 18.2 If the MAC fails to comply with a SAR, the requester may apply for a court order requiring the MAC to comply or to seek compensation. It is a matter for the court to decide, in each particular case, what action to take.

19. What Happens If the Requestor Is Not Happy with Their SAR Response

- 19.1 In the first instance, the requestor should raise their concern with the MAC. The MAC should take the complaint seriously and work with the requestor to try to

resolve it. However, if no resolution is found, the requestor then has the right to raise a concern with the ICO.

- 19.2 If the ICO think the MAC have not responded to the request appropriately, the ICO can give the MAC advice and ask them to resolve the problem.

20. Response times

- 20.1 Requests received under the Data Protection Act need to be responded to within one month upon the day of receipt of the request (for example, a SAR received on 3 September should be responded to by 3 October). Requests can be made verbally or in writing. The time limit can be extended by up to a further 2 months where a request is complex. If an extension to the time limit is required, the requestor will need to be informed within one month at the latest.
- 20.2 Requests received for Educational Records need to be responded to within 15 school days upon receipt of the written request.
- 20.3 If a request is received that involves both personal information and educational records the information must be provided within 15 school days.
- 20.4 The deadline for responding continues throughout the school holiday periods for SARs. Therefore, it is important the office@ email account and social media accounts are monitored for any requests. Using the excuse of the school being closed is not acceptable with the ICO for SARs.

21. Retention

- 21.1 Please ensure that you keep a copy of the information that you have sent out in response to a request as the requestor may ask for a review to take place if they are not happy with the response. A copy of the response needs to be kept for 3 years and then it can be securely destroyed.

Appendix 1 – Data Protection Checklist

<p>DATA PROTECTION SAR CHECKLIST</p> <p>TO HELP WITH COMPLIANCE PLEASE COMPLETE THE LIST BELOW BEFORE SENDING ANYTHING OUT</p>	
Please go through the list below and tick to confirm you have ENSURED THAT:	√
You have read the question(s) and fully understand what is being requested -	
The information has been put in date order as far as possible -	
No third-party information will be disclosed inappropriately – <i>(Also - consider carefully the circumstances where staff names are disclosed and seek advice if unsure)</i>	
Redacted material cannot be seen e.g., when held up to the light –	
Only the information asked for has been disclosed –	
Any information likely to cause measurable harm and distress has not been disclosed inappropriately –	
Where the requestor is acting on behalf of a third party, there is documented evidence of authority to act on behalf of that third party -	
Appropriate checks have been made with any third parties providing information before disclosure -	
Where there is Medical/Health data, necessary checks have been made with the relevant medical/health professional before disclosing -	
All necessary ID checks have been made before disclosure -	
Where appropriate, fees have been asked for/obtained -	
Any information already made available to the requestor is included, only where appropriate –	
Any documents referred to are included and/or explained –	
Any codes or abbreviations included are explained –	

The information relates to the requestor, and he/she has not been confused with anyone else –	
You have taken further advice where you are unsure about disclosing anything –	
You have checked and removed any unnecessary duplicate material –	
You have appropriately disclosed all information as required by the SAR -	
The information will only be disclosed via an appropriate and secure method, with all necessary management information about the request clearly recorded –	
A record/copy of what has been sent is retained-	