MK College Group

Building

Fairer Futures.

Data Subject Access Request Policy

Author:	Data Protection Officer
Date:	Thursday, 25 September 2025
Version:	Version 1.3
Review requirements:	Biennially
Date of next review:	September 2027
Approval body:	GLT 16 September 2025
Checked by:	Executive Head of IT, Group Director for People Services
Publication:	College Intranet / Website

This policy and procedure is subject to The Equality Act 2010 which recognises the following categories of individual as Protected Characteristics: Age, Gender Reassignment, Marriage and Civil Partnership, Pregnancy and Maternity, Race, Religion and Belief, Sex (gender), Sexual orientation, Disability.

MK College Group

Contents

Definitions

Key words in this document are defined as follows

- MUST: This word, or the terms “REQUIRED” or “SHALL”, mean that the definition is an absolute requirement.
- MUST NOT: This phrase, or the phrase “SHALL NOT”, mean that the definition is an absolute prohibition.
- SHOULD: This word, or the adjective “RECOMMENDED”, mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- SHOULD NOT: This phrase, or the phrase “NOT RECOMMENDED” mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood, and the case carefully weighed before implementing any behaviour described with this label.
- MAY: This word, or the adjective “OPTIONAL”, mean that an item is truly optional.

Scope

- This policy applies to all requests for access to individual personal data, whether received from them directly, or from another person with appropriate authority.

Purpose

- To assist staff in responding to subject access requests.
- To comply with the obligations described in the UK GDPR and Data Protection Act 2018
- To safeguard and protect the students and staff and their personal data

Related Legislation

- Data (Use and Access) Act 2025 (https://www.legislation.gov.uk/ukpga/2025/18/contents)

- Data Protection Act 2018
  (https://www.legislation.gov.uk/ukpga/2018/12/contents)
- General Data Protection Regulation (EU 2016/679)
  (https://www.legislation.gov.uk/eur/2016/679/contents)
- The Equality Act 2010
  (https://www.legislation.gov.uk/ukpga/2010/15/contents)

Data Subject Access Request Procedure

Introduction

The UK General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA), as amended by the Data (Use and Access) Act 2025, provide individuals with rights in connection with the personal data held about them. It provides those individuals with a right of access to their data, subject to the rights of third parties and the satisfaction of a number of criteria, and right to correct information held about them. This procedure defines the process to be followed when a request for access to personal data or correct personal data is received.

Reference documents

- Data (Use and Access) Act 2025 (Commencement No. 1) Regulations 2025
- UK-GDPR (United Kingdom General Data Protection Regulation) January 2020.
- Data Protection Act 2018
- Milton Keynes College Data Protection Policy
- Milton Keynes College Data Retention Policy
- Milton Keynes College Safeguarding Policies
- DPO Tracker

Responsibilities and definitions

- **Data Protection Officer** (DPO) is responsible for ensuring that statutory and regulatory obligations with respect to the Data Protection Act and GDPR are adhered to. Where DPO is referred to, they may nominate a 'responsible person' to undertake some of their actions in regard to this procedure.
- **Employees** are responsible for incorporating this procedure and its associated policy into their own working practices.
- **Data Subject** is the person whose data is being requested
- **Data Subject Representative** is an authorised person who is requesting information about or on behalf of the data subject
- **Data Subject Access Request (DSAR)** is any request made by an individual or an individual's legal representative for information held by the College about that

individual. The DSAR provides the right for data subjects to see or view their own personal data as well as to request copies of the data.

Data subject rights

The rights to data subject access include the following:

- To know whether a data controller holds any personal data about them.
- To receive a description of the data held about them and, if permissible and practical, a copy of the data.
- To be informed of the purpose(s) for which that data is being processed, and from where it was received.
- To be informed whether the information is being disclosed to anyone apart from the original recipient of the data; and if so, the identity of those recipients.
- The right of data portability. Data subjects can ask that their personal data be transferred to them or a third party in machine readable format (Word, PDF, etc.). However, such requests can only be fulfilled if the data in question was provided by the data subject to the College, is processed automatically and is processed based on consent or fulfilment of a contract.
- If the data is being used to make automated decisions about the data subject, to be told what logic the system uses to make those decisions and to be able to request human intervention.

Much of this information is provided data subjects via the relevant College Privacy Notices.

The College must provide a response to data subjects requesting access to their data within **One Month** of receiving a valid DSAR. This period may be extended under some circumstances, for example where the information requested is complex and includes sensitive information or information related to other parties. The volume of information held may also be a factor for consideration but is ordinarily not sufficient in its own right to warrant an extension.

Where proof of identity, or other information or clarification on the request are required, the period permitted for response is paused, and days elapsed between a request for proof of identity or clarification and the provision of that proof or clarification, do not count towards the applicable time period.

Requests

Requests for correction of data

Requests for correction of data may be actioned once the validity of the request is verified.

- For staff, many changes to personal information can be processed in Buddy, our employee self-service platform. Other change requests should be sent to the People Services team.

- For students, most requests to update contact details and personal information can be sent to the MIS team, who will verify the identity of the requestor and ensure that the request is appropriate

Gender, Pronoun and Names

- Where a change in data is requested due to a change in gender-identity, the college LGBTQIA Policy explicitly supports adoption of the pronouns, gender marker and name that an individual requests be used, and such requests should be actioned on receipt: see Safeguarding Policies and Procedures

Marriage, Divorce and Name Change

- Sometimes change in name or surname may arise from a change in circumstance on the part of the student or member of staff, or their families. This can include marriage, divorce, or a personal decision. Where the change is requested by the data subject themselves, these can be dealt with as ordinary business.
- Sometimes a request for a change of name can be accompanied by a formal notarised statement renouncing the previous name (unenrolled deed poll), or formal notice that the change in name is to be published at the Royal Courts (enrolled deed poll). Enrollment of the deed poll is not required. Persons under the age of 16 may have a deed poll submitted on their behalf. Persons over the age of 16 should submit a deed poll on their own behalf. https://www.gov.uk/change-name-deed-poll

- Where a change is requested by another party; e.g. a parent asking on behalf of their son or daughter, we should seek confirmation that the data subject is consenting to the change. Where we receive an objection to a name change from a third party, for example a parent or other family member, the wishes of the data subject take precedence.
- If you have any concerns regarding a request for a change in name, please contact the Data Protection Officer as soon as possible.
- If you are concerned that a change in name has been requested due to coercion or is made under duress, please alert your line manager and/or the Safeguarding team as soon as possible.

Academic Grades and Attainment

- Where a request is made to change a recorded grade or attainment, specific care must be taken that there is adequate evidence that the college record is genuinely in error.
- Right to Rectification is not an appropriate route to challenge properly recorded grades or attainment, regardless of whether the grade or attainment itself is in dispute. Where a grade or attainment has been disputed, and a decision has been made to change that grade or attainment, the college record should be updated to reflect that change as soon as possible.

Bank and Payroll Information

- Requests to change bank account information, change pension contributions, or other payroll related information, should be passed to the Payroll team. These requests will be actioned as soon as possible, but where a request is received in the days approaching the monthly payroll batch run, it may be delayed until after the payroll run has been actioned.
  Many changes to staff information can be enacted by staff themselves via the HRIS platform self-service interface (currently this is Buddy, accessed via the staff intranet)

Other information corrections and changes

- If you receive a request for information to be updated or changed, and either it is unclear if the request is from the data subject, you are unable to verify the

identity of the data subject, or you are unsure who is responsible for the data that being updated, please contact the Data Protection Officer as soon as possible.

Subject Access Requests

The GDPR does not specify how to make a valid request. Therefore, an individual can make a subject access request verbally or in writing, including on social media. It can also be made to any part of the College (including by social media) and does not have to be to a specific person or contact point. A request is valid if it is clear that the individual is asking for their own personal data. An individual does not need to use a specific form of words, refer to legislation or direct the request to a specific contact.

Staff should be careful to ensure that barriers are not put into place that prevent data subjects making access requests, and that any processes comply with Equality Act obligations.

Upon receipt of a DSAR, employees must transfer the request to the DPO (or nominated deputy), who will acknowledge the request.

The date of the initial request and the request details should be logged in the 'DPO Tracker with a unique case reference number.

NOTE:
If there is any doubt as to the identity of the requestor, and either proof of identity or proof of delegated authority are required, the one month response period starts the day the data subject/requestor submits valid proof of identity or delegated authority that has been verified (see paragraph 18).

If clarification of the request, or further information from the requestor is required, the days between the request and the receipt of clarification or the further information are not counted in regard to the period prescribed for a response to be provided

If it is clear that the information being requested is 'complex or numerous' then the period of compliance may be extended for a further two months. In these circumstances the College must inform the data subject within one month of receipt of the request and explain why the extension is necessary.

Request for data held under a contract

Requests relating to data that is “owned” by other organisations acting as Data Controller, and where the college acts as a Data Processor on their behalf (e.g Prison Education contracts), shall be referred to that organisation, and the requestor informed that this has been done. Contracts and partnership agreements should specify the nature of the data relationship between parties and include explicit clauses that define such obligations.

Identity verification

The DPO needs to check the identity of anyone making a DSAR to ensure information is only given to the person who is entitled to it.

In the case of a request from current staff or students, the submission of the request through their verified email address may be enough. Generally, however, there will be a requirement for the data subject and requestor (if relevant) to provide identification. This should be a government issued document containing a photo and/or a signature, or a verified contact channel and sufficient personal information provided as to satisfy the DPO as to the identity of the requestor. This may include full name, full address, date of birth and student Id or staff payroll numbers.

If the requestor is not the data subject, written confirmation that the requestor is authorised to act on behalf of the data subject is required, as well as validating the requestors’ identity.

If valid identification is not sent within a reasonable time period (provided the College is confident that the request was delivered and has undertaken reasonable follow-up to ensure the data subject does not wish to pursue their right) the case should be closed and the response logged.

Gathering information

The DPO will contact relevant staff and provide them with the DSAR.

Staff should consider where 'personal data' about the individual concerned might be held and conduct a search. Information may be stored electronically or in hard copy. It may be located in databases, filing systems (electronic and manual), student or personnel records, shared drives, the Intranet, College Social media accounts, email and/or filing systems of particular individuals, or with third party service providers. If necessary, colleagues may need to search their personal drives and e-mail accounts.

The college IT department may assist in searching the email server and storage drives for the name of the requestor.

The Data Use and Access Act 2025 Section 78 has amended Article 15.1 of the UK GDPR, and clarified that :

- *Under paragraph 1, the data subject is only entitled to such confirmation, personal data and other information as the controller is able to provide* ***based on a reasonable and proportionate search*** *for the personal data and other information described in that paragraph.*

Information discovered should be relayed to the DPO electronically by email or shared electronic folder. Physical documents may be scanned and emailed securely or copied and sent via secure mail. The DPO may meet with staff to review progress and offer advice if required.

A folder in Outlook on the DPO mailbox should be created for each DSAR – the filename should be made up from the reference number and surname of the applicant and should contain:

- Copies of the correspondence between the DPO and the data subject and between the DPO and any other parties.
- A record of any methods used to verify the identity of the data subject.
- A record of the DPO decisions and how they came to those decisions.
- Copies of the information sent to the data subject, including any anonymised or redacted versions sent.

A Working Folder should be created to hold copies on files awaiting review and redaction, and a sub-folder for that data which is prepared for release.

Guidance on what constitutes personal data is contained in Appendix 1.

If no personal data is found then the DPO should be informed. A written response to that effect will be sent to the data subject/representative and the response logged.

Review of information

The DPO will determine whether there is any information which may be subject to an exemption and/or if consent is required to be provided from a third party identified within the information (see section 6). Further guidance on how to review information is contained in Appendix 2.

The DPO must ensure that the information is received and reviewed in time to ensure the one month timeframe is not breached, or that the need to extend the deadline by two months has been identified and relayed to the requestor, and that the extended deadline is not breached.

A DSAR relates to the data held at the time the request was received. It is not acceptable to amend or delete the data if we would not otherwise have done so. Under the DPA, it is an offence to make any amendment with the intention of preventing its disclosure.

Response

The DPO will provide the finalised response together with the information retrieved from the department(s) and/or a statement that the College does not hold the information requested, or that an exemption applies. This response must be logged.

The DPO will ensure that a written response will be sent back to the requestor. This will be via email, unless the requestor has specified another method by which they wish to receive the response (e.g. post). The College will only provide information via channels that are relatively secure. When hard copies of information are posted, they will be sealed securely and sent by recorded delivery.

Exemptions

An individual does not have the right to access information recorded about someone else, unless they are an authorised representative, or have explicit permission held on record (e.g a parent where the student has completed a consent form identifying that they are permitted ongoing access to the student information).

The College is not required to respond to requests for information unless it is provided with sufficient details to enable the location of the information to be identified, and to satisfy itself as to the identity of the data subject making the request.

In principle, the College will not normally disclose the following types of information in response to a DSAR:

- Information about other people – A DSAR may cover information which relates to an individual or individuals other than the data subject. Access to such data will not be granted, unless the individuals involved consent to the disclosure of their data. (See Appendix 3 for further details)
- Repeat requests – Where a similar or identical request in relation to the same data subject has previously been complied with within a reasonable time period, and where there is no significant change in personal data held in relation to that data subject, any further request made within a six month period of the original request will be considered a repeat request, and the College will not normally provide a further copy of the same data.
- Publicly available information – The College is not required to provide copies of documents which are already in the public domain.
- Opinions given in confidence or protected by law – The College does not have to disclose personal data held in relation to a data subject that is in the form of an opinion given in confidence or protected by law.
- Privileged documents – Any privileged information held by the College need not be disclosed in response to a DSAR. In general, privileged information includes any document which is confidential (e.g. a direct communication between a client and their lawyer) and is created for the purpose of obtaining or giving legal advice.
- If the information is kept only for the purpose of statistics or research, and where the results of the statistical work or research are not made available in a form that identifies any of the individuals involved.
- Requests made for other, non-data protection purposes
- Vexatious requests

If the DPO refuses a DSAR, the reasons for the rejection must be clearly set out in writing. Any individual dissatisfied with the outcome of their Data Subject Access Request is entitled to make a request to the College to review the outcome.

Documentation and Retention

Records of responses relating to a subject access request may be retained for up to 6 years.

Appendix 1: What is personal data?

The GDPR applies to the processing of personal data that is:

- wholly or partly by automated means; or
- the processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system.

Personal data only includes information relating to living natural persons who:

- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.
- Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive, and you may only process them in more limited circumstances.
- Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.
- If personal data can be *truly* anonymised, then the anonymised data is not subject to the GDPR. It is important to understand what personal data is to understand if the data has been anonymised.
- Information about a deceased person does not constitute personal data and therefore is not subject to the GDPR.
- Information about companies or public authorities is not personal data.
- However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information relates to them as an individual may constitute personal data.

Appendix 2: Reviewing information

What can, and cannot, be disclosed as a result of a DSAR

Once all the information held about a data subject has been collected, it must be examined in detail to establish if it should be disclosed. This must be done on a case-by-case basis for each individual piece of information. In some cases, only parts of documents should be disclosed.

It is the information and not copies of the documents that are legally required to be disclosed.

The below points must all be taken into consideration, subject to the relevant interest and balance tests as prescribed by legislation and guidance from the ICO

- Check that the record is about the person concerned and not about someone else with the same name. Just because a record contains somebody's names does not always mean that it is about them. For example, an e-mail might carry the subject line "Meeting about John Smith" but if the e-mail only contains details about whether people can attend the meeting, the e-mail is not about John Smith.
- Screen out duplicate records. For example, if there has been an e- mail exchange between colleagues, it is only necessary to print out the last e-mail in the exchange if copies of all the other e-mails are part of the last e-mail.
- If a record was created by a member of staff acting in a private rather than an official capacity, only exceptional circumstances would justify its disclosure without their consent. If they are not prepared to disclose the record, do not disclose it. A classification of private capacity may be influenced by the context in which the record was created, the persons it has been shared with (if any) and the subsequent use of or reference to the record by the creator and any other third party. Staff should be cautious of records or information created in regard to students or other staff, as it is the use and reference to it that will decide whether it can be lawfully withheld, not the channel/platform on which it was created.
- The College should only disclose information which is about the person making the subject access request. Where a document contains personal data about a number of individuals, including the data subject, they should not disclose the information about the third parties to the data subject. If the record is primarily

about the data subject, with incidental information about others, they should redact the third-party information. If the record is primarily about third parties, withhold it if redacting is not possible. Alternatively, contact the third party to obtain consent to disclose the document if possible. Ensure that all correspondence in these matters is logged.

- The records may contain correspondence and comments about the data subject from several parties, including private individuals, external individuals acting in an official capacity, and College staff. In these cases, we are required to balance the interests of the third party against the interests of the data subject and often omit or redact third party information. Third party data exemptions may not apply in cases where there is no legitimate expectation of privacy; staff should expect to be identified in documents and records relating to students, or where they occupy a senior position, or significant decision-making position, in relation to the data subject.
- Do not disclose information which would prejudice the prevention or detection of a crime. For example, if the Police informed us that a member of staff is under investigation, but the member of staff did not know this, then we should not provide that information to the member of staff whilst the investigation is in progress. However, if the investigation is closed or if the member of staff has been informed that there is an investigation underway, then the information should be disclosed in response to a subject access request.
- Do not disclose any records which contain advice from our lawyers, where we are asking for legal advice or which were written as part of obtaining legal advice unless there are exceptional circumstances.
- Do not disclose information that is being used, or may be used in future, in negotiations with the data subject if the information gives away our negotiating position and disclosing the information would weaken that negotiating position unless there are exceptional circumstances.

The exemptions identified above are those most likely to apply to information held by the College. There are others, and it is good practice to check the Information Commissioners Office website for up-to-date information regarding exemptions before responding to a DSAR. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/ . Advice should be sought when it is thought that another exemption may be applicable.

If the DPO discovers material which does not reflect favourably on the College (e.g. they may find documents which show that standard procedures have not been followed, or documents which may cause offence to the data subject), these documents must still be disclosed. However, the DPO should bring their contents to the attention of the relevant manager and ensure that appropriate action is taken to address any issues that may arise.

Staff MUST NOT destroy or refuse to disclose records. This is a criminal offence if it is done after you know a subject access request has been made.

Once all the information that can be sent in response to a DSAR has been collated, one final review of this information as a collection must be made. This is to offset the risks often discovered by aggregating information. For example, the DPO may have identified that all the information they intend to release is unrestricted in its nature. However, once aggregated there is an inherent risk that additional information could be disclosed or at least interpreted. This must be taken into consideration before the final response is made.

Appendix 3: Third Party Information

Responding to a subject access request may involve providing information that relates both to the individual making the request and to another individual. However, the DPA 2018 says that organisations do not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information, the College must, however, take into account all of the relevant circumstances, including:

- the type of information that you would disclose;
- any duty of confidentiality you owe to the other individual;
- any steps you have taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

So, although the College may sometimes be able to disclose information relating to a third party, it needs to decide whether it is appropriate to do so in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the College disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the College must decide whether to disclose the information anyway. For the avoidance of doubt, the College cannot refuse to provide access to personal data about an individual simply because it has obtained that data from a third party.

The rules about third party data apply only to personal data which includes both information about the individual who is the subject of the request and information about someone else.