Myddelton College

Data Protection Policy and Procedures

Policy produced by	HT	
Date policy reviewed and approved	March 2023	
Reviewed and approved by	Headteacher LDA plus SLT Nov 2024	
Next review due	Nov 2025	
Published on website	**Yes**	No

Contents

DATA PROTECTION IN SCHOOLS

Department for Education 3 Feb 2023 (updated August 2024)

Data protection in schools - Guidance - GOV.UK

DATA PROTECTION POLICY AND PROCEDURES

1. **Introduction:**

In order to carry out our statutory, academic and administrative functions, Myddelton College collects and processes the personal data of:

a. staff,
b. pupils and their parents and/or guardians,
c. other stake holder groups.

2. **Our commitment:**

The College takes confidentiality of all personal data very seriously, taking every reasonable step to comply with: United Kingdom General Data Protection Regulation, and Data Protection Act 2018.

The College will only collect personal data to meet specifically planned, agreed and necessary purposes, and will keep it no longer than is necessary.

3. **Definitions:**

a. Data protection legislation refers to the United Kingdom General Data Protection Regulation or GDPR.
b. Personal data is information relating to an identified person.
c. Data controller refers to the person controlling the use of personal data; the College is a data controller.
d. A data processor is a person who processes data for the data controller.
e. A data subject is an individual whose personal data is held by the college.
f. The processing of data refers to its collection, recording, re-organisation, storage, and use.
g. A data subject access request refers either to a person's right of access to their personal data.
h. A data breach refers to a breach of security leading to the accidental or unlawful loss of a person's or group's data.

4. **Key Principles:**

Personal Data is

- processed fairly, lawfully and transparently;
- collected only for specific purposes;
- kept accurate with the College taking responsible steps to ensure it remains so (inaccurate data will be rectified without delay);
- not kept for longer than is necessary;
- kept securely.

The College informs individuals both why their personal data is needed and how it will be used.

5. **Data protection responsibilities:**

a. Data controllers implement this policy;
b. Directors monitor this policy, ensuring it is implemented as required;

c. The Headteacher is responsible for applying strict safeguards to the processing of personal data;
d. The College will take all reasonable measures to ensure:
   - personal data is collected, held, processed and disposed of in a secure way,
   - those wanting to access their personal data are made aware of the process,
   - data subject access requests are dealt with efficiently,
   - staff are made understand their duties under Data Protection Legislation,
   - staff are made of the College's policies and procedures,
   - methods of processing personal data are reviewed annually,
   - GDPR requirements are considered when new policies and systems are created or updated;
e. Staff will support the data controllers by complying with all data protection instructions, and this Policy. A breach of these could result in disciplinary action.

6. Staff and middle managers' responsibilities:

When handling confidential or sensitive information about, for example, pupils' coursework, making judgements as to ability in relation to achievements, contributing to reports or references, or considering details of pupils' personal circumstances, staff must:

- keep information secure - locked away, encrypted or password protected;
- hard copies of pupils' personal data, if taken off site, must be held securely;
- only access personal data they have authority to access;
- not share or communicate this data without permission;
- not disclose by any means, either accidentally or unintentionally others' personal information, to include 'phone calls, emails or casual comments.

7. Staff, Pupils, Parents, Directors responsibilities:

- checking information provided is accurate and current;
- informing the College of any changes to personal data;
- checking the accuracy of personal data regularly;
- correcting errors promptly.

8. Data Processors are responsible for:

- co-operating in terms of having a written Data Processing Agreement in place;
- processing personal data in accordance with data protection;
- ensuring colleagues are made aware of and fulfil their responsibilities under Data Protection legislation;
- assist with data subject access requests and reporting and correcting data breaches;
- provide information on how personal data is processed, how it can be accessed, and how it can be corrected or rectified;
- supporting any requests for deletion or removal of personal data, to include blocking or suppressing its processing;
- allowing individuals to obtain and re-use personal data for their own purposes;
- supporting the right to object to the processing of personal data;
- stopping automated decision making and profiling of personal data on request.

9. **Parents and pupils requesting changes in personal data:**
   Parents or pupils can make requests for data change as follows:
   - requests should be submitted to the College Office (Headteacher's PA);
   - these should be made either in writing (letter or email preferably) or submitted on paper in person, giving:
     the original and incorrect personal data, the corrected personal data, and
     a signature, with date, of the person(s) whose personal data requires change.

10. **Staff requesting changes in personal data:**

Staff members are asked to put their requests for changes in personal data on paper and hand these in person to the Headteacher's PA.

11. **Right of Access to personal data:**

Data subjects have the right under the UK's GDPR to obtain confirmation as to whether their personal data is being processed by the College and access has been given without approval. To exercise this right, requests must be made in writing to the Headteacher via their PA. These will be dealt with quickly and certainly within one month of the request.

Requests which cannot be fulfilled: there is no automatic right of access to personal data if it contains data exempt from the right of access. Such data or information might, for example, include and/or identify third parties or be legally privileged information.

The right to erasure is limited as the College might have compelling reasons to refuse specific requests to delete data; this might be, for example, in order to comply with a legal or safeguarding requirement, or if there are overriding legitimate grounds. All such requests will be considered on their own merits.

12. **Children's Rights over their Personal Data:**

Rights, under UK GDPR, relate to the individuals to whom the Personal Data refers. However, the law recognises children's rights to have a say over how their Personal Data is used from the age of 13.

Myddelton College, in the majority of cases, will rely on parental consent to process personal data relating to pupils unless, given the nature of the processing in question, and the pupil's age and understanding, it is unreasonable in all circumstances to rely on the parent's consent. Parents should be aware that, in such situations, they may not be consulted.

If a young person is deemed incapable of making their own decisions, a parent or guardian will act on their behalf. This authority is only extended to functions that are 'in the best interests of the child'.

Where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds agreement to personal data being disclosed to a parent or guardian, Myddelton College will maintain
confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding consent, or where the College believes disclosure will be in the best interests of the pupil or other pupils.
Where opinions regarding the use of a pupil's personal data conflict between the pupil and the parent, the College will make every effort to reach a solution in which both parties are content.

13. Data Security:

Disclosure of Personal Data
Myddelton College may receive requests from third parties to disclose personal data. On the majority of occasions, the College will not disclose information unless the individual has either given consent, or it is to be disclosed for a legitimate business interest, for example:

- providing a reference to an educational institution;
- disclosing public examination results or other achievements;
- providing details of a medical condition without which the pupil's best interests are not served;
- receiving a disclosure request from a third party - (here the college will seek the DSP's view on the appropriateness of such actions).

14. International Data Transfer:

All pupils, staff members and other individuals who handle college data must not transfer personal data outside the UK without first consulting the data compliance officer.

Myddelton College has a duty of care to put adequate safeguards in place, where reasonably possible, to protect such data.

15. Data Retention:

Data will be wiped or deleted as soon as it is no longer important to retain it. A typical time period would be within the first three months.

16. Data Protection Registration:

The College is a data controller; as such, Myddelton College is required by the Information Commissioner's Office to be registered on their Data Protection Public Register (https://ico.org.uk/esdwebpages/search). The Information Commissioner's Office acts as the UK regulator for data protection purposes.

17. Queries and/or Complaints:

Myddelton College will handle queries and/or complaints relating to the processing of personal data promptly. These should be raised in the first instance with the Headteacher, via their PA.

Should you wish to refer the matter to the Information Commissioner's Office (ICO), you should make contact: 0303 123 1113, or https://ico.org.uk/make-a-

complaint/.

18. Policy Review

This policy will be reviewed by the Senior Leadership Team every two years or following a breach of security, or receipt of a complaint.

Taken from:

Data Protection in Schools

From: Department for Education Published: 3 February 2023

The policies and processes Schools and multi-academy trusts need to protect personal data and respond effectively to a personal data breach.

1. Introduction:

Good data protection practices ensure that an organisation and the individuals within it can be trusted to collect, store and use our personal data fairly, safely and lawfully.

All those who process others' personal data have to follow strict rules. These rules are set primarily by: the UK General Data Protection Regulation (UK GDPR)
the Data Protection Act 2018 (DPA)

2. Data processing a School is permitted to do:

The lawful grounds for accessing, collecting, storing and using personal, special category and criminal offence data: Under data protection legislation, there are a number of justifications that permit personal data to be processed. It's important to remember that a justification relates to the processing activity and not to the data itself, so a
justification has to be established for each activity.

3. Responsibilities:

Everyone in your School is responsible for protecting personal data. There are some key roles and responsibilities for data protection compliance.

The data controller:

For most of the personal data you collect, store and use, the School or the multi-academy trust is the data controller.
This means it's responsible under the Data Protection Act 2018 for protecting data in every situation where it decides:

whose information to
collect what types of data
it needs why it needs it
whether the information can be shared with a third
party when and where data subjects' rights apply
for how long to keep the data

As a data controller, your School needs to register with the Information Commissioner's Office.
Where, for example, a School is required to supply a copy of some personal data to the Department for Education (DfE), DfE also becomes an independent data controller of the copy it receives.

4. Data protection policies and procedures:

How to comply and document compliance with UK GDPR and the Data Protection Act 2018.

Under UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA),
Schools have to: comply with the legislation
demonstrate that they're complying

You can read more about the personal data you need to document and how to do so on the Information Commissioner's Office (ICO) website.

5. **Statutory policies:**

It's a legal requirement that your School has data protection policies and procedures in place and that you regularly review and update these, along with the associated documentation. You should also review your other statutory policies in the light of data protection legislation.

6. **Record of processing activities:**

A record of processing activities is an efficient means of capturing all the important information about your School's data processing activities. It will improve your information governance and show your compliance with accountability principles. It will also ensure you comply with other aspects of data protection law, such as the requirement to create privacy notices and keep personal data secure, thereby reducing the risk of a personal data breach.

Step 1: identify your personal data assets:

Locate all the personal data your School has received, created or shared. It could be stored

in: management information systems
communication systems
safeguarding technology
health and social care records
systems curriculum management
software virtual learning
environments workforce systems
catering systems
equipment records
photo and video storage systems
paper records and photos
statutory returns to the Department for Education (DfE) and local authorities

Step 2: list your personal data assets:

Compile a list of that personal data. Start with broad data item groups, then add beneath each group specific data items. For example, the data item groups for pupils might be:

admissions
attainment
attendance
behaviour
exclusions
personal identifiers, contacts and pupil characteristics
identity management and authentication
catering and free School meal management trips
and activities
medical information and administration
safeguarding and special educational needs

Repeat this for the personal data assets of all data subjects in the School community.

Step 3: add information about your personal data assets:

Record extra detail about each of the personal data items in the list. There's no definitive format you need to follow in creating your record of processing activities, so develop your own to suit your School's needs, using this guidance as a starting point.

Mandatory information
Your record of processing activities should include the following as a
minimum: the name and contact details of your School
the name and contact details of your data protection officer (DPO)/data
protection lead the name and contact details of any joint controllers
the purposes of the personal data processing you
carry out the categories of personal data you process
the categories of individuals whose personal data you process
the categories of organisations with which you share
personal data the schedule for retaining each category of
personal data
a general description of your technical and organisational security measures

Additional information:
The following prompts will help you add more detail about each personal data item to your record of processing activities.
Source of personal data
Record whether the data item:
was received by the
School was created by
the School
has been or will be shared by the School
Category of personal data
Record whether it's:
personal data
special category
data criminal
offence data
Data controller or data processor
Record whether, in respect of this data item:
the School's a data controller or a data processor
the School's a joint controller and, if so, with which organisation
there's an up-to-date controller-processor contract in place, if
applicable Access and use
Record, in respect of this data item:
the lawful basis (personal data) and, if applicable, additional condition (special category or
criminal offence data) that allows it to be accessed and used
who has access to it and how that's controlled
whether there's an up-to-date data sharing agreement in place, if
applicable Data retention and destruction
Record, in respect of this data item, the:
data retention period and the justification for it
procedure for depersonalisation or disposal of it at the end of the retention period
disposal is manual or automated and, if manual, there's a prompt to ensure it is
destroyed Consent, rights and subject access requests
Record whether, in respect of this data item, data subjects
have: given their consent for it to be processed and, if
so, how
been informed of their rights regarding access, rectification and erasure

been told about the procedure for making a subject access request Security and personal data breaches

Record whether, in respect of this data item, there:

are up-to-date information and communication technology (ICT) security policies and procedures in place to prevent a cyberattack

is a procedure for secure sharing

is a procedure for handle a personal data breach Automated decision-making

Record whether, in respect of this data item, the processing involves any automated decision-making.

Share your record of processing activities with your School leadership team (SLT) and Directors or trustees. They are responsible for ensuring your School is compliant with the DPA and keeps only the personal data it needs.

7. Sharing personal data:

Who you can share personal data with and what consent you need to get – for example, when publishing exam results and taking photos in School.

To keep children and young people safe in School, you need to share information appropriately, so the correct decisions can be made to protect them.

You must have a compelling reason to share their personal data. Sharing children's data with third parties can expose them to unintended risks if not done properly. You should carry out a data protection impact assessment to assess any risk before sharing personal information about your pupils.

The Information Commissioner's Office has a data sharing information hub that includes further guidance on data sharing. Any data you share must comply with their data sharing code of practice.

8. Safeguarding:

To keep children safe and make sure they get the support they need, you can share information with other Schools and children's social care teams. It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child.

Your designated safeguarding lead will decide if personal data needs to be shared. They should make sure they record:

who they're sharing that information

with why they're sharing the data

whether they have consent from the pupil, parent or carer

Read 'Working Together to Safeguard Children' to find out more information about sharing a pupil's safeguarding file. You should also refer to the safeguarding section of 'Keeping Children Safe in Education' (2022).

9. Sharing data with local authorities and government:

Occasionally, you may need to share personal information about your pupils with local authorities, other Schools or children's services. For example:

if a pupil shows signs of physical or mental abuse, you may need to pass this information on to children's services

another School may need to know which pupils will be at their sports day or on a joint School trip

Sharing information can help provide appropriate services that safeguard and promote the welfare of children. The Data Protection Act 2018 and UK GDPR provides a framework to make sure that personal information is shared appropriately.

Before you share any data, you must:

consider all the legal implications
check if you need permission to share the data
confirm who needs the data, what data is needed and what they'll use it for make sure that you have the ability to share the specified data securely
check that the actions cannot be completed or verified without the data

You also have a statutory requirement to share personal data about your pupils with DfE through the School census.

You do not need to get consent from pupils, parents or carers to share this data with us. You should provide information about what data you share in your School's privacy notice. Privacy notice model documents suggest wording to explain to staff, parents, carers and pupils what data you're collecting and sharing.

Schools may also need to share personal data about their staff with the local authority.

10. **Sharing data with other Schools:**

If a pupil moves to another School, you should transfer their records to the new School. This includes the pupil's common transfer file and educational record. You must:

make sure you transfer the data securely
transfer the record within 15 days of getting confirmation the pupil is registered at another School be able to trace the record during the transfer

To securely share and transfer pupil records, you

could: use the School to School (S2S) system
send them to a named person using an encrypted email ask your local authority to transfer them
deliver any paper records in person or ask the new School to collect them

If you're organising a School trip with another School, you'll need to share data with them to confirm which pupils are going. You may also need to share details such as dietary requirements or medical information to make sure pupils
are safe. Where you already have consent for the information, make sure this also covers sharing it.

11. **What you need consent for:**

Before sharing any personal data, you usually need consent from the individual. There may be some circumstances where it may not be appropriate to ask for consent, however. For example:

if the individual cannot give consent it's not reasonable to ask for consent when there's a safeguarding concern
You'll usually need to get the pupil's consent to share their data if they're aged 13 or over. If they're under 13, you must get consent from whomever holds parental responsibility for the child.

Guidance on understanding and dealing with issues relating to parental responsibility is also available. The
Information Commissioner's Office has guidance to help you understand a child's rights over their personal data.

12. **How to get consent:**

You can get consent in different ways. It must be clear that the individual agrees to share their personal data and understands what they're agreeing to. Do not use pre-ticked boxes or add disclaimers that by not responding they are agreeing to share their data. You should keep a record of:

- the consent
- when you got the consent
- how you got the consent – for example, keeping the letter you sent to parents or carers

When getting consent, you need to explain:

what personal information you're
sharing why you're sharing it
who you're sharing it with and what they'll use it
for how you'll share their information
the process for withdrawing consent

Any letters you send to parents or carers that ask for a reply slip that includes personal data should have a data protection statement. This could mean linking to a privacy notice or including information within the letter.

If you're asking for consent from a pupil aged 13 or over, you must write your request so they can understand it and are clear about what they're agreeing to.

Case study: ensuring data subjects have their rights respected when using biometric data
If you use pupils' biometric data as part of an automated biometric recognition system, such as using
fingerprints to receive School meals instead of paying with cash, you must comply with the requirements of the Protection of Freedoms Act 2012.
That means following these steps.

In accordance with the child's age or capacity, get written consent from at least one parent or carer before you take and process any biometric data from their child. See the section on consent over age of 13.
Provide an alternative means to access the relevant services for any pupil from whom you do not have consent. For example, pupils must be able to pay for School meals using cash at each transaction, if they wish.
Delete any relevant data already captured, if a parent or carer withdraws their consent.
If a pupil does not want their biometric data processed, you must not process it even if their parent or carer has given consent. This is required by law.
You also need to get consent from any staff members using the School's biometric system. Staff can withdraw their consent at any time and you must then delete any relevant data already captured.
Guidance is available on protecting children's biometric information in School.

13. Taking and using photos in School:

Photos are used in School for many different reasons. You'll need consent for each different use of a photograph. You must get consent to:

share photos on your School's social media channels
include photos of pupils and staff in your prospectus or other marketing
material use a photo of a pupil in your School displays
take a photo for a newspaper article

If you're using a photo of a pupil, do not include their name unless you have specific consent to do so.
You should only use a photo in line with the consent provided. When you're asking for consent, you should make it clear for how long you'll use the photograph.
Photos used in identity management systems may be essential for performing the public task of the School, but you should delete them once a child is no longer a pupil at your School.
The Information Commissioner's Office provides further guidance on taking photos in School.

14. Publishing exam results:

UK GDPR does not stop Schools from publishing exam results online or in the local press.
You do not need to get consent from pupils, parents or carers to publish exam results. However, you should tell pupils where and how their results will be published before they're published. This gives

them an opportunity to ask you to remove their results from the list should they wish to.
The Information Commissioner's Office has more information about exam results and data protection.