Mendip Edge Federation

Data Protection Policy

Includes Subject Access, Freedom of Information,
Data Breach Reporting and Data Retention Procedures

Contacts

Data Protection Officer:	Amy Brittan dposchools@somerset.gov.uk
School Data Protection Leads:	Cheddar First School: Margaret Wookey cheddarfirst@educ.somerset.gov.uk
	Draycott & Rodney Stoke First School: Mike Jory sch.137@educ.somerset.gov.uk
	Shipham First School: Mike Jory sch.301@educ.somerset.gov.uk
	Fairlands Middle School: Oliver Crandon office@fairlandsmiddleschool.co.uk

Introduction

The Mendip Edge Federation (MEF or Federation) needs to collect, store and use information about pupils, staff and other individual in order to fulfil its educational duties. The MEF may also be required to provide other parties with data where it has a legal, statutory, legitimate or contractual right to do so.

The Federation will comply with the data protection principles set out in the Data Protection Act 2018 (DPA) and all other laws.

The Data Controller and Other Roles

The four schools of the Federation are Data Controllers.

The Federation has appointed Amy Brittan of Support Services for Education as its designated Data Protection Officer[1].

Other day to day matters will be dealt with by each school's Data Protection Lead[2] and Headteacher.

[1] Appendix A: *Role of the Data Protection Officer*
[2] Appendix B: *Role of the Data Protection Lead*

Responsibilities of the Schools

The schools are committed to protecting and respecting the confidentiality of personal information relating to staff, pupils, parents and governors. The schools will:

- Register with the Information Commissioners Office (ICO)
- Keep an up-to-date Data Asset Audit[3], which lists all known uses of personal data in the school
- Ensure that all systems involving personal data or confidential information meet the DPA regulations
- Inform all users about their rights regarding data protection through privacy notices, available on each school's website
- Provide training to ensure that staff (including volunteers) know their responsibilities
- Monitor its data protection and information security processes on a regular basis, changing practices if necessary
- Securely dispose of data when it is no longer required to be held.

Responsibilities of Staff (Including Volunteers)

Each school will have a procedure in place for staff to follow, to ensure data protection practice is in line with the DPA.

All staff are responsible for checking that any information they provide to the schools is accurate and up-to-date.

All staff are responsible for ensuring that any personal data they use in the process of completing their role:

- Is not in the view of others who do not have the authority to view the data
- Is kept securely in a locked cabinet when not being used
- Is stored on a secure local or network drive
- If kept on removal storage (laptop, tablet, memory stick) approved by the school, the devices must be password protected and encrypted. The individual is responsible for ensuring this data is backed up regularly
- Is not disclosed to any unauthorised third party
- Is assessed and approved by the school's DPL and Senior Leadership Team, with advice from the DPO where necessary, if used within an app or web service.[4]

Staff should note that unauthorised disclosure of data, or a transgression of the above statements, may result in disciplinary action.

[3] Appendix C: *Data Asset Audit*
[4] Appendix D: *Privacy Impact Assessment*

Responsibilities of Parents/Carers

The schools will inform parents/carers of the importance of keeping personal data provided to the school up-to-date. This process will include at least an annual data collection sheet (with the return of this document being recorded) and reminders in newsletters and at parents' evenings or meetings.

Schools will also seek permissions regarding matters of non-statutory use of personal data, such as the use of images and names in publicity materials, on induction or as required. The returns to these permissions will be recorded and exemptions communicated to staff.

Rights to Access Information

Anybody having personal data stored by the schools has the right to obtain confirmation if personal data concerning themselves, or their child, is being processed.

Where this is the case, they have the right to have a copy of the personal data and the following information:

- The purpose of the processing
- The third parties that the data will be shared with
- The period for which the personal data will be stored
- The right to request the schools to correct, erase or restrict processing of personal data, if the data can be proved to be held incorrectly
- The right to lodge a complaint with a supervisory authority
- Where the personal data is not collected from the data subject, any available information as to its source.

If exemptions are placed on any of the data above, because of safeguarding or other issues, the existence of this data will be declared.

The schools will place privacy notices on their websites regarding the personal data held about their learners and workforces, and the reasons for which it is processed.

Where a data subject or parent/guardian wishes to request a copy of the relevant personal data, this subject access request should be made in writing to either the Headteacher or the Chair of Governors.

The process for handling subject access requests can be found here.[5]

The Federation aims to comply with requests for access to personal information as quickly as possible, and in accordance with guidance from the ICO.

Freedom of Information Requests

[5] Appendix E: *Process for handling Subject Access Requests*

As required by the Freedom of Information Act, each school of the Mendip Edge Federation will publish a *Freedom of Information Publication Scheme* on its website. All information included within the scheme will be published accordingly.

Freedom of Information requests are requests from any member of the public about processes, policies and other non-personal information about the school. These requests will always be processed and the rights of individuals not to be identified (within the DPA) will be respected, while maintaining legal responsibilities within the Freedom of Information Act.

The process for dealing with Freedom of Information requests is outlined in the Process for Handling Freedom of Information Requests.[6]

Data Breaches

If there is a data breach, the relevant school's DPL will inform the DPO.

Any data breaches will be recorded, comprising the facts relating to the personal data breach, its effects and the remedial action taken, as explained in the Data Breach Process.[7]

If there are risks to the data subject/s, the school will communicate the breach to those affected.

In the case of a personal data breach, the ICO will be informed as soon as possible and within 72 hours of notification. Further investigation of the breach can take place after this notification, in line with advice from the DPO and the ICO.

Data breaches are reported using the information provided by the ICO.[8,9]

[6] Appendix F: *Process for handling Freedom of Information Requests*
[7] Appendix G: *Data Breach Process*
[8] https://ico.org.uk/for-organisations/report-a-breach/
[9] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Data Retention Policy

In accordance with the DPA, each school has responsibilities to keep data for only as long as necessary. The Mendip Edge Federation uses the Data Retention Schedule provided by the Information and Records Management Society's Records Management Toolkit for Schools.
Any paper records due for destruction will be cross-cut shredded, either by the relevant school or an appropriately authorised external company. Data held on electronic devices will be deleted in line with ICO advice.

A record will be kept of all data destroyed and/or the certificate of destruction issued by a third party.

Reporting Policy Incidents

Any member of staff, parent or other individual who consider that this Policy has not been followed in respect of personal data should raise the matter with the Headteacher or Chair of Governors.

Monitoring and Evaluation

This policy will be monitored and reviewed at intervals no longer than 2 years or in response to changes in regulations or events.

Appendix A: Role of the Data Protection Officer

Purpose

The Data Protection Officer (DPO) is responsible for monitoring compliance with current data protection law, and has the knowledge, support and authority to do so effectively. They oversee and verify the school's data protection processes and advise the school on best practice.

Data Protection Officer Responsibilities

To:

- advise the school about their obligations under the Data Protection Act 2018;
- maintain, with the DPL, a joint understanding of the school's processing operations, information systems, data security processes and needs, and administrative rules and procedures;
- ensure monitoring of the school's compliance with data protection law, by:
    - collecting information to identify data processing activities;
    - analysing and checking the compliance of data processing activities;
    - informing, advising and issuing recommendations to the school;
    - ensuring they have current and detailed information in data protection issues and changes to the law, attending relevant training as appropriate;
- make sure that the school's policies are followed, through:
    - assigning responsibilities to individuals;
    - awareness-raising activities;
    - coordinating staff training;
    - conducting internal data protection audits;
- advise on and assist the school with carrying out data protection impact assessments, if necessary;
- act as a contact point for the ICO, assisting and consulting it where necessary, including:
    - helping the ICO to access documents and information;
    - seeking advice on data protection issues;
- act as a contact point for individuals whose data is processed (for example, staff, pupils and parents), including:
    - responding with support from the DPL to subject access requests;
    - responding with support from the DPL to other requests regarding individuals' rights over their data and how it is used;
- take a risk-based approach to data protection, including:

    - prioritising the higher-risk areas of data protection and focusing mostly on these
    - advising the school if/when it should conduct an audit, which areas staff need training in, and what the DPO/DPL roles involve.
- report to the governing board/board of trustees on the school's data protection compliance and associated risks;
- respect and uphold confidentiality, as appropriate and in line with data protection law, in carrying out all duties of the role;
- assist the DPL in maintaining a record of the school's data processing activities;
- work with external stakeholders, such as suppliers or members of the community, on data protection issues;
- working with the DPL in fostering a culture of data protection throughout the school;
- work closely with other departments and services to ensure DPA compliance, such as HR, legal, IT and security;
- work with the Senior Leadership team at the school to ensure DPA compliance;
- assist with any additional tasks necessary to keep the school compliant with data protection law and be successful in the role.

Tasks

From these responsibilities, isolated tasks should include:

- providing a model Data Protection Policy and assist in customising it for the school;
- advising on procedures and pro formas to allow the Data Protection Policy to be adhered to;
- providing advice on other associated policies and documents;
- providing materials and advice in completing a dynamic Data Asset Audit and assisting in its completion if necessary;
- collecting the Data Asset Audit on a yearly basis and checking for issues;
- providing training materials to allow the DPL to assist staff in keeping up to date with Data Protection issues;
- acting as the point of contact for SAR and FOI requests and supporting the school to provide the information as required;
- providing a Data Protection Audit on a 3 yearly rota basis and producing a report for Governors;
- providing telephone and email advice and support;
- providing regional training for the DPL and other staff;

- providing school based on-demand training either as part of the Ed Tech subscription or at cost.

Appendix B: Role of the Data Protection Lead

Purpose

Within each school there will be a Data Protection Lead (DPL), who maintains contact with the DPO and is responsible for assisting in monitoring with compliance and verifies the school's data protection practices on a day to day basis.

Data Protection Lead Responsibilities

To:

- maintain the school's registration with the ICO;
- support the DPO in advising the school about their obligations under the Data Protection Act 2018;
- support the DPO in developing an understanding of the school's processing operations, information systems, data security processes and needs, and administrative rules and procedures;
- assist the DPO with the monitoring of the school's compliance with data protection law, by:
    - collecting information to identify data processing activities;
    - analysing and checking the compliance of data processing activities;
    - informing, advising and issuing recommendations to the school;
    - ensuring they have current and detailed information in data protection issues and changes to the law, attending relevant training as appropriate;
- assist the DPO in making sure that the school's policies are followed, through:
    - assigning responsibilities to individuals;
    - awareness-raising activities;
    - coordinating staff training;
    - conducting internal data protection audits;
- act as a contact point for the DPO in supporting individuals whose data is processed (for example, staff, pupils and parents), including:
    - responding with support from the DPO to subject access requests;
    - responding with support from the DPO to other requests regarding individuals' rights over their data and how it is used;
- maintain the school's Data Asset Audit as a record of the school's data processing activities and provide this on a yearly basis to the DPO;
- assisting the DPO in working with external stakeholders, such as suppliers or members of the community, on data protection issues;
- working with the DPO in fostering a culture of data protection throughout the school;

- work with the Senior Leadership team at the school to ensure DPA compliance;
- assist with any additional tasks necessary to keep the school compliant with data protection law and be successful in the role.

Tasks

From these responsibilities, isolated tasks should include:

- act as the school's primary point of contact with the DPO and for all matters relating to data protection;
- assist in customising the Data Protection Policy for the school;
- advising on procedures and pro formas to allow the Data Protection Policy to be adhered to;
- provide advice on other associated policies and documents;
- sourcing materials, information and advice to complete and maintain the school's Data Asset Audit;
- supplying the DPO with the Data Asset Audit on a yearly basis;
- using the training materials provided by the DPO to assist the staff in keeping up to date with Data Protection issues.

Appendix C: Data Asset Audit

Each school will document the personal data it stores.

These documents will be dynamic documents and be the responsibility of the DPLs, assisted by the DPO. They will be updated using the Privacy Impact Assessment forms completed by staff.

The documents will be completed using the template provided by the DPO.

Data Asset Audit

Description of service	Type of data	Reason to hold data	Where is data stored?	Is the data shared with anyone?	Risks

Date: _____

Checked by:_____

dposchools@somerset.gov.uk

Appendix D: Privacy Impact Assessment Template

Privacy Impact Assessment (PIA) for:

Name of Service/Software/App

Data Protection Principles

- processing to be lawful and fair
- purposes of processing be specified, explicit and legitimate
- adequate, relevant and not excessive
- accurate and kept up to date
- kept for no longer than is necessary
- processed in a secure manner

Why we need a Privacy Impact Assessment – screening questions?

We need to complete this form because:

- the use involves the collection of new information about individuals;
- the use compels individuals to provide information about themselves;
- the information about individuals will be disclosed to organisations or people who have not previously had routine access to the information;
- we are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- we are using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition;
- the use results in you making decisions or acting against individuals in ways that can have a significant impact on them;
- the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private;
- the use requires you to contact individuals in ways that they may find intrusive.

Describe the service

Describe the data collected and the possible uses of the data

List of data held	**Collection of data**
	Possible uses

Identify the privacy, related risks and possible solutions To be discussed with the Data Protection Lead

Privacy issue	Risk to individuals	DPA Risks	Possible Solutions
1.	•	•	•
2.	•	•	•
3.	•	•	•
4.	•	•	•
5.	•	•	•
6.	•	•	•

Sign off and notes

Comments on risks	Processes that must be in place

Contact point for future privacy concerns

Data Protection Officer: dposchools@somerset.gov.uk

Data Protection Lead: A Person - aperson@educ.somerset.gov.uk

Date completed: Automatically generated

Appendix E: Process for Handling Subject Access Requests

On receiving a Subject Access Request or request for change or deletion of data, the DPO or school will:

- inform the DPL in the school (and the Headteacher if necessary);
- record the details of the request, updating this record where necessary (see next page);
- reply to the requestor informing receipt of the request asking for clarity if there is confusion about which data is required;
- contact the DPO if clarity on the request is needed or procedure is needed;
- identify the people responsible for gathering the necessary data;
- gather the data indicating a deadline;
- examine the data for redactions making sure there is no ‘bleeding’ of data;
- ask the requestor for an address and time for delivery.

The whole process should take no longer than **30 calendar days**, which can be extended by a further 2 months where the request is complex or where there are numerous requests.

Please note the time for processing a request for an Educational Record is **15 days**.

Subject Access Request Record Template

Name of data subject: _____

Name of person who made request: _____

Date request received: ____/____/____

Contact DPO (dposchools@somerset.gov.uk) : ____/____/____

Date acknowledgement sent: ____/____ /____

Name of person dealing with request: _____

	Notes (Overwrite the statements in grey)
Are they entitled to the data?	If no reply stating reasons and/or ask for proof
Do you understand what data they are asking for?	If no, ask requestor for clarity
Identify the data	What data sources, where they are kept
Collect the data required	You may need to ask others – state a deadline in your request.
Do you own all the data?	If no, ask third parties to release external data. If data is supplied by another agency such as Psychology Service, you do not own the data.
Do you need to exempt/redact data?	If exempting/redacting be clear of your reasons Document name, data exempted/redacted, why.
Is the data going to be ready in time?	Record delays and reasons. Communicate with requestor stating reason for delay and asking if they would like the data you have collected so far.
Create pack	Make sure that the data is in an easy to access format: paper, word, excel etc.
Inform requestor you have the data	Ask them how they would like it delivered
Deliver data	Ask for confirmation/special delivery?

At all stages, your DPO or DPL will be able to provide you with advice.

Date request completed: ____/____/____

(within 30 days of request)

Signed off by: _____

Appendix F: Process for Handling Freedom of Information Requests

On receiving a Freedom of Information Request, which must be made in writing, the DPO or the school will:

- inform the DPL in the school (and the Headteacher if necessary);
- record the details of the request, updating this record where necessary (see next page);
- reply to the requestor informing receipt of the request asking for clarity if there is confusion about which data is required;
- decide that if the material is already published or falls within an exemption;
- contact the DPO if clarity on the request is needed or procedure is needed;
- if data is not going to be published inform the requestor why this is not being released;
- identify the people responsible for gathering the necessary data;
- gather the data indicating a deadline;
- examine the data for redactions making sure there is no ‘bleeding’ of data;
- ask the requestor for an address and time for delivery.

The whole process should take no longer than **20 working days**.

Freedom of Information Request Record Template

Name of person who made request: _____

Date request received: ____/____/____

Contact DPO (dposchools@somerset.gov.uk) : ____/____/____

Date acknowledgement sent: ____/____ /____

Name of person dealing with request: _____

	Notes (Overwrite the statements in grey)
Are they entitled to the data?	If no reply stating reasons
Do you understand what data they are asking for?	If no, ask requestor for clarity
Identify the data	What data sources, where they are kept
Collect the data required	You may need to ask others – state a deadline in your request.
Do you own all the data?	If no, then refer them to the correct agency
Do you need to exempt/redact data?	Could the data identify individuals Are any of the answers less than 5 people – use '5 or less including zero)? Are their commercial sensibilities?
Is the data going to be ready in time?	Record delays and reasons. Communicate with requestor stating reason for delay and asking if they would like the data you have collected so far.
Create pack	Make sure that the data is in an easy to access format: paper, word, excel etc.
Inform requestor you have the data	Ask them how they would like it delivered
Deliver data	Ask for confirmation/special delivery?

At all stages, your DPO or DPL will be able to provide you with advice.

Date request completed: ____/____/____

(within 20 days of request)

Signed off by: _____

Appendix G: Data Breach Process

Every Data Protection Breach should be recorded. The process that should be followed is listed below:

- inform the DPL in the school (and the Headteacher if necessary);

- record the details of the breach providing these details:

    - a description of the nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned; and
    - the categories and approximate number of personal data records concerned;
    - the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
    - a description of the likely consequences of the personal data breach; and
    - a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

- contact the DPO if clarity on reporting the breach is needed and if necessary report to the ICO;

    - either by phoning 0303 123 1113
    - By filling in the form at: https://ico.org.uk/media/for-organisations/documents/2258298/personal-data-breach-report-form-web-dpa-2018.doc and sending it to casework@ico.org.uk

- updating this record where necessary (see next page);

- identify the people whose data is accidentally released, inform them of the breach and the processes taken to rectify the situation;

- review why the breach took place and if future similar events can be avoided.

Data Breach Record Template

Date: / /	Person responsible for dealing with breach				
Description of the nature of the personal data breach including, where possible:					
The categories and approximate number of individuals concerned					
The categories and approximate number of personal data records concerned					
A description of the likely consequences of the personal data breach					
A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects					
Reported by					
Phone/email sent to DPO dposchools@somerset.gov.uk	y/n	Is this high risk?	y/n	Report to ICO	y/n
Date reported to data subjects					
Notes					
Actions approved by		Date	/ /		