

Data Protection Impact Assessment (CPOMS)



The Fosse MAT operates a cloud based system or 'hosted solution' called CPOMS. Access to CPOMS is through the internet. Resources are retrieved from CPOMS via the Internet, through a web-based application, as opposed to a direct connection to a server at the school. Access to CPOMS can be through a PC, smartphone, iPad and tablet. As such The Fosse MAT must consider the privacy implications of such a system. The Data Protection Impact Assessment is a systematic process for identifying and addressing privacy issues and considers the future consequences for privacy of a current or proposed action.

The Fosse MAT recognises that using a 'hosted solution' has a number of implications and recognises the need to have a good overview of its data information flow..

The Data Protection Impact Assessment is a systematic process for identifying and addressing privacy issues and considers the future consequences for privacy of a current or proposed action. The Fosse MAT recognises that moving to a cloud service provider has a number of implications. The Fosse MAT recognises the need to have a good overview of its data information flow.

The Data Protection Impact Assessment looks at the wider context of privacy taking into account Data Protection Law and the Human Rights Act. It considers the need for a cloud based system and the impact it may have on individual privacy.

The school needs to know where the data is stored, how it can be transferred and what access possibilities the school has to its data. The location of the cloud is important to determine applicable law. The Fosse MAT will need to satisfy its responsibilities in determining whether the security measures the cloud provider has taken are sufficient, and that the rights of the data subject under the GDPR is satisfied by the school.

The Fosse MAT aims to undertake this Data Protection Impact Assessment on an annual basis.

A Data Protection Impact Assessment will typically consist of the following key steps:

1. Identify the need for a DPIA.
2. Describe the information flow.
3. Identify data protection and related risks.
4. Identify data protection solutions to reduce or eliminate the risks.
5. Sign off the outcomes of the DPIA.

Step 1 Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

What is the aim of the project? – CPOMS is a software application which enables The Fosse MAT I to improve their management of child protection and similar incidents and actions, whilst reducing staff time, paperwork and administration.

CPOMS is an intuitive system to help with the management and recording of child protection, behavioural issues, bullying, special educational needs, domestic issues and more. CPOMS contains sensitive information within an electronic format which is held securely on a remote server.

CPOMS also enables the school to track referrals to external agencies, such as NHS/CAHMS, Children's Services, and the Police (including letters and phone calls) and to be alerted if timescales are not being met.

This same functionality enables The Fosse MAT to track communication with parents and carers, as well as the students themselves. A meeting held, conversation with a child, or a decision to undertake an Early Help Assessment can all be recorded on the system, in a safe, secure and searchable method.

To record sensitive pupil information electronically which is password protected will help mitigate against the risk of a data breach with the appropriate controls in place.

CPOMS has a Privacy Notice which states that for the purposes of IT hosting the information may be located on servers within the European Union.

The Fosse MAT will undertake the following processes:

1. Collecting personal data
2. Recording and organizing personal data
3. Storing personal data
4. Copying personal data
5. Retrieving personal data
6. Deleting personal data

By opting for CPOMS the school aims to achieve the following:

1. Management of sensitive pupil information in one place
2. Security and integrity of sensitive data through a secure document vault
3. Storage of information electronically rather than manually
4. Recording information and building a chronology around the pupil
5. Alerting staff and setting up reminders as appropriate
6. Providing bespoke reports for difference audiences, e.g. Governors or Ofsted
7. Tracking vulnerable groups and identifying trends
8. Ability to add information from staff across the school
9. Secure access across all devices wherever the setting

Cloud based systems enable the school to upload documents and other files to a hosted site to share with others within school. These files can then be accessed securely from any location or any type of device (laptop, mobile phone, tablet, etc).

CPOMS cannot do anything with the school's data unless they have been instructed by the school. The schools Privacy Notice will be updated accordingly.

The Fosse MAT has included CPOMS within its Information Asset Register.

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

The Privacy Notices (pupil) for the school provides the legitimate basis of why the school collects pupil data. Specifically this relates to health and safety and safeguarding of vulnerable groups

How will you collect, use, store and delete data? – CPOMS collects information from behavior and attendance records, Special Educational Needs (SEN) records, Education Health Care Plans (EHCP), Safeguarding records and from other sources. CPOMS links into Brook Primary School Management Information System drawing pupil data into the application. The information will be stored on CPOMS. The information is retained according to the school's Data Retention Policy.

What is the source of the data? – Attendance and behavior information, Safeguarding files, SENCO records, Education Health and Care Plans, Pupil Records, and Common Assessment Framework.

Will you be sharing data with anyone? – The Fosse MAT may share information with safeguarding professionals including the Designated Safeguarding Lead, SENCO, headteacher, Senior Leadership Team (SLT), Governors, Ofsted, the local authority, i.e. Safeguarding Children Board, Local Authority Designated Officer (LADO), Social Services, the NHS/CAHMS, the Police, according to agreed safeguarding procedures. However, this does not mean that The Fosse MAT School shares CPOMS access to the third parties.

What types of processing identified as likely high risk are involved? – The information is transferred securely from the school to the server which is hosted remotely on a server within the European Union. Access to information on CPOMS is controlled through passwords, with additional security to the most sensitive information. For example, the Designated Safeguarding Leads and Headteacher would have access to the most sensitive information using a two tiered log in procedure. Other members of staff would only have access to report incidents on CPOMS.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

What is the nature of the data? – Pupil data relates to the name of the child, date of birth, and class. Data also includes attendance and behavior information and SEN. Names of other agencies involved, i.e. NHS/CAHMS, counselling, early help, speech and language therapists, health visitors, social workers, and details of outcomes. CPOMS contains electronic records of the work of the School in dealing with a suspected/actual safeguarding issue and monitor progress and outcomes.

To create a ClassDojo account as a teacher or school leader information required includes first and last name, e-mail address, telephone number, password and a profile photograph.

Special Category data? – Data revealing racial or ethnic origin, and religious beliefs are collected by the school and contained in CPOMS. The lawful basis for collecting this information relates to Article 9 2 (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorized by domestic law (see section 10 of the 2018 Act) or a collective agreement pursuant to domestic law providing for appropriate safeguards for the fundamental rights and interests of the data subject.

How much data is collected and used and how often? – Personal details relating to pupils are obtained from parent/pupil information systems. Safeguarding content obtained from classroom/teacher observation/agency partners. This also includes recorded information and reports.

How long will you keep the data for? –The school follows the good practice in terms of data retention as set out in the IRMS Information Management Toolkit for Schools. Safeguarding information is transferred to the receiving school as part of the pupil record. This is signed for by the receiving school. This is then kept by the receiving school from DOB of the child + 25 years then reviewed. This retention period has also been agreed in consultation with the Safeguarding Children Board on the understanding that the principal copy of this information will be found on the Local Authority Social Services record.

Scope of data obtained? – How many individuals are affected (pupils, workforce, governors, and volunteers)? And what is the geographical area covered?
Reception to Year 6 (120) Workforce (17) Board of Governors (6)

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

What is the nature of your relationship with the individuals? – The Fosse MAT collects and processes personal data relating to its pupils to ensure the school provides education to its students with teaching staff delivering the National Curriculum.

Through the Privacy Notice (Pupil/Workforce) The Fosse MAT is committed to being transparent about how it collects and uses data and to meeting its data protection obligation.

How much control will they have? – Not all staff will have access to safeguarding information. CPOMS can restrict access to the designated persons file and restrict access to searching information on the system. Access to the data held on CPOMS will be controlled by username and password.

Additionally whilst CPOMS works on any device with access to the internet, those members of staff with higher levels of access to sensitive information must download an Authenticator App which provides additional security with access to additional sensitive information. For the password to be accepted, an alphanumeric combination with special characters must be used for the system to accept. It also has the functionality to have an automatic time out facility set by The Fosse MAT.

Access to CPOMS can be revoked at any time. If a member of staff hasn't logged in, in excess of 60 days, the login will need to be reactivated and a new password set. As a default, passwords must be changed every 60 days.

The school will be able to upload personal data from its PC for the data to be stored remotely. Any changes made to files are automatically copied across and immediately accessible from other devices the school may have.

Do they include children or other vulnerable groups? – All of the data will relate to children. The information will relate to safeguarding, health plans, pupil attendance and behavior, etc.

Are there prior concerns over this type of processing or security flaws? – Does the cloud provider store the information in an encrypted format? What is the method of file transfer? For example, the most secure way to transfer is to encrypt the data before it leaves the computer. Encryption does have its limitations inasmuch as the encryption key will need to be shared with others to access the data.

The Fosse MAT recognises that moving to a cloud based solution raises a number of General Data Protection Regulations issues as follows:

ISSUE: The cloud based solution will be storing personal data including sensitive information

RISK: There is a risk of uncontrolled distribution of information to third parties.

MITIGATING ACTION: CPOMS uses a two factor authentication process, password and key required for higher access

ISSUE: Transfer of data between the school and the cloud

RISK: Risk of compromise and unlawful access when personal data is transferred

MITIGATING ACTION: All data is encrypted from source and in transit (from the management information system to CPOMS) to the data centre and back again to the data controller

ISSUE: Understanding the cloud based solution chosen where data processing/storage premises are shared?

RISK: The potential of information leakage

MITIGATING ACTION: It may be appropriate for the school to consider the use of encryption on data 'at rest', i.e. when stored in the cloud service. This will be an important consideration when sensitive data is being processed

ISSUE: Cloud solution and the geographical location of where the data is stored

RISK: Within the EU, the physical location of the cloud is a decisive factor to determine which privacy rules apply. However, in other areas other regulations may apply which may not be Data Protection Law compliant

MITIGATING ACTION: Data centres are in the UK (owned by Memset). This means that the GDPR privacy rules apply to the cloud based service

ISSUE: CPOMS as a third party processor and privacy commitments respecting personal data, i.e. the rights of data subjects

RISK: GDPR non-compliance

MITIGATING ACTION: It is advisable that the school tailor any contract to incorporate these privacy commitments

ISSUE: Implementing data retention effectively in the cloud

RISK: GDPR non-compliance

MITIGATING ACTION: School to take into consideration backups and if the data is stored in multiple locations and the ability to remove the data in its entirety

ISSUE: Responding to a data breach

RISK: GDPR non-compliance

MITIGATING ACTION: The school will recognize the need to define in their contract a breach event and procedures for notifying the school and the school managing it

ISSUE: Subject Access Requests

RISK: The school must be able to retrieve the data in a structured format to provide the information to the data subject

MITIGATING ACTION: Providers will need to provide the technical capability to ensure the school can comply with a data subject access requests. This may be included as part of the contract

ISSUE: The right to be informed; the right of access; the right of rectification; the right to erasure; the right to restrict processing; the right to data portability; the right to object

RISK: The school is unable to exercise the rights of the individual

MITIGATING ACTION: Providers will need to provide the technical capability to ensure the school can comply with such requests. This may be included as part of the contract

ISSUE: Data Ownership

RISK: GDPR non-compliance

MITIGATING ACTION: The school must maintain ownership of the data and this should be included in the contract

ISSUE: Cloud Architecture

RISK: The school needs to familiarise itself with the underlying technologies the cloud provider uses and the implications these technologies have on security safeguards and protection of the personal data stored in the cloud

MITIGATING ACTION: The data is stored in tier 3 data centres

ISSUE: GDPR Training

RISK: GDPR non-compliance

MITIGATING ACTION: Appropriate training is undertaken by personnel

ISSUE: Security of Privacy

RISK: GDPR non-compliance

MITIGATING ACTION: CPOMS is ISO 9001 and ISO 27001 registered

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

The school moving to a cloud based solution will realise the following benefits:

1. Management of sensitive pupil in one place
2. Security and integrity of sensitive data through a secure document vault
3. Storage of information electronically rather than manually
4. Recording information and building a chronology around the pupil
5. Alerting staff and setting up reminders as appropriate
6. Providing bespoke reports for different audiences, e.g. Governors or Ofsted
7. Tracking vulnerable groups and identifying trends
8. Ability to add information from staff across the school
9. Secure access across all devices wherever the setting

Step 3 Consultation Process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

The views of senior leadership team and the Board of Governors will be obtained. Once reviewed the views of stakeholders will be taken into account

The view of YourIG has also been engaged to ensure Data Protection Law compliance

Step 4 Access necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

The lawful basis for processing personal data is contained in the school's Privacy Notice (Pupil and Workforce). The Legitimate basis includes the following:

- Childcare Act 2006 (Section 40 (2)(a))
- The Education Reform Act 1988
- Further and Higher Education Act 1992,
- Education Act 1994; 1998; 2002; 2005; 2011
- Health and Safety at Work Act
- Safeguarding Vulnerable Groups Act
- Working together to Safeguard Children Guidelines (DfE)

The school has a Subject Access Request procedure in place to ensure compliance with Data Protection Law

The cloud based solution will enable the school to uphold the rights of the data subject?
The right to be informed; the right of access; the right of rectification; the right to erasure; the right to restrict processing; the right to data portability; the right to object; and the right not to be subject to automated decision-making. The school will continue to be compliant with its Data Protection Policy

Step 5 Identify and assess the risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
Data transfer, data could be compromised	Possible	Severe	Medium
Asset protection and resilience	Possible	Significant	Medium
Data Breaches	Possible	Significant	Medium
Subject Access Request	Probable	Significant	Medium
Data Retention	Probable	Significant	Medium

Step 6 Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks

Risk	Options to reduce and eliminate risk	Effect on risk	Residual risk	Measure approved
		Eliminate, reduce, accepted	Low, medium, high	Yes/no

Data transfer	Secure network, end to end encryption	Reduced	Medium	Yes
Asset protection and resilience	Data centre in EU, certified, Penetration Testing and Audit	Reduced	Medium	Yes
Data breaches	Documented in contract and owned by schools	Reduced	Low	Yes
Subject Access Request	Technical capability to satisfy data subject access request	Reduced	Low	Yes
Data retention	Implementing school data retention periods in the cloud	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Sam Welsby January 2025	Integrate action back into project plan, with date and responsibility for completion
Residual risks approved by:	Sam Welsby January 2025	If accepting any residual high risk, consult yore ICO before going ahead
DPO advice provided:	Yes	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Do not need to obtain parental consent to be added to system as there is a legitimate interest to using ClassDojo (homework could be shared through the system).		
DPO advice accepted or overruled by:	Yes	If overruled, you must explain your reasons
Comments		
Consultation responses reviewed by:		If you decision departs from individuals' views, you must explain your reasons
Comments		
This DPIA will be kept under review by:	Sam Welsby, Tim Hewitt, Paige Allister and Sarah Eadon	The DPO should also review ongoing compliance with DPIA