

Data Protection Impact Assessment (Reach More Parents)



The Fosse MAT operates a cloud based system or 'hosted solution 'called Reach More Parents.

Access to Reach More parents is through the internet. Resources are retrieved from Reach More Parents via the Internet, through a web-based application, as opposed to a direct connection to a server at the school. Access to Reach More Parents 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? – To help deliver a cost effective solution to meet the needs of the business. The cloud based system will enable the school to contact those with parental responsibility in a timely and efficient way.

Reach More Parents is first and foremost a communication platform, helping schools share and retrieve information. Reach More parents can be accessed by the user via mobile devices.

There is an expectation that parents will be updated in a timely manner about anything that will impact upon their child whilst they are at the school. The most appropriate method to provide parents with this information is via Reach More Parents which will ensure that important messages are delivered to parents without reliance on the pupil.

The school may, for example, post details of school closure on its website or via a local radio station. However, there is no guarantee that this information may reach those with parental responsibility in a timely manner.

The text messaging service will only be used to inform parents of school activities and issues which may impact on the child. Consent has been identified as the lawful basis for processing personal data in the The Fosse MAT Privacy Notice (Pupil).

Reach More Parents has a Privacy Notice which states that for the purposes of IT hosting the information may be located on servers within the UK.

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 Reach More Parents 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.

Brook Primary School 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

6.1 (c) Processing is necessary for compliance with a legal obligation to which the controller is subject; e.g. health & safety and safeguarding

6.1 (e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

6.1 (f) Processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party

The school has highlighted consent as the lawful basis by which it processes personal data.

This is recorded in The Fosse MAT Privacy Notice (Pupil). The school needs to determine what lawful basis it intends to use. If there is real choice then consent is appropriate and if there is no choice then a legitimate interest assessment would be appropriate.

How will you collect, use, store and delete data? – The information collected by the school is retained on the school's management information system. Reach More Parents also collects information from online contact forms, import of data from the school management information system, verbal and written from nominated administrator contact within the school. The information is retained according to the school's Data Retention Policy.

What is the source of the data? – Pupil information is collected via registration forms when pupils join the school, pupil update forms the school issue at the start of the year, Common Transfer File (CTF) or secure file transfer from previous schools.

Will you be sharing data with anyone? – The Fosse MAT routinely shares pupil information with relevant staff within the school, schools that the pupil attends after leaving, the Local Authority, the Department for Education, Health Services, Learning Support Services, RM Integrus and various third party Information Society Services applications.

What types of processing identified as likely high risk are involved? – Transferring personal data from the school to the cloud. Storage of personal data in the Cloud

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 personal identifiers and contacts (such as name and their school groups – classes, years, etc).

The Privacy Policy for Reach More Parents states that the following personal data will be collected: The names of students and their school groups (classes, years etc.); the names of any parents, guardians, carers or other student contacts along with their mobile phone numbers and email addresses; and the names of staff members and their mobile phone numbers.

The school will ensure that it has the authority to share data with Reach More Parents on behalf of the school; it has obtained the lawful basis to provide the personal information of any individual to Reach More Parents and have obtained all necessary consent to contact any individual through the Services (via the Reach More Parents application, or by email or SMS). It also states under the 'data minimization' principle that Reach More Parents will never collect any unnecessary personal data from the school and will not process school information in any way, other than that specified in the Privacy Notice for Parent Hub.

The information is sourced from the individual schools from the management information system either via manual import or automated transfer.

Special Category data? – None of the personal data collected falls under the GDPR special category data. This includes race; ethnic origin; religion; biometrics; and health. These may be contained in the Single Central Record, RM Integris, child safeguarding files, SEN reports, etc.

How much data is collected and used and how often? – Personal data is collected for all pupils and their respective parent/guardians. Additionally personal data is also held respecting school administrative contact details, school name and address, school e-mail address, school contact telephone number, and staff information (staff name, staff e-mail address, staff teaching groups).

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? – Reach More Parent users (students, parents, staff) may have individual user accounts to log into Parent Hub to retrieve communications. Passwords are not stored, a hashed representation of the password is created and associated with the account.

Do they include children or other vulnerable groups? – None of the data is classified under GDPR as special category. However, personal data will be collected: pupil information including the pupil name, pupil UPN (unique pupil number), and pupil class name.

Are there prior concerns over this type of processing or security flaws? – Reach More Parents does not rely on old fashioned in house servers, as they are fully cloud-hosted on the Amazon Web Services UK data centre.

Reach More Parents all criteria set out in the DfE's cloud supplier checklist, and are on the UK Government G-Cloud list of approved cloud suppliers. They store, process and manage your personal data in the UK. Data is encrypted using industry standard AES-256 and TLS1.3 protocols.

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: Reach More Parents secure identity server encrypts user access credentials that are required to access Reach More Parents.

A username and password must be entered to access any part of Reach More Parents. Each user requires a unique username and password. In the event an account is compromised the school is able to deactivate the affected account. The school can choose which staff are able to access Parent Hub and assign different roles to those staff members, thus managing which staff have access to the data within Parent Hub

ISSUE: Transfer of data between the school and the cloud

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

MITIGATING ACTION: Amazon Web Services UK data centre.

Reach More Parents all criteria set out in the DfE's cloud supplier checklist , and are on the UK Government G-Cloud list of approved cloud suppliers. They store, process and manage your personal data in the UK. Data is encrypted using industry standard AES-256 and TLS1.3 protocols.

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

RISK: The potential of information leakage

MITIGATING ACTION: Amazon Web Services UK data centre.

Reach More Parents all criteria set out in the DfE's cloud supplier checklist , and are on the UK Government G-Cloud list of approved cloud suppliers. They store, process and manage your personal data in the UK. Data is encrypted using industry standard AES-256 and TLS1.3 protocols.

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 Amazon). This means that the GDPR privacy rules apply to the cloud based service

ISSUE: Implementing data retention effectively in the cloud

RISK: GDPR non-compliance

MITIGATING ACTION: When a school requests its data to be deleted, Reach More Parents, unless prohibited to do so by law, will delete the data. However, even after deletion, all information will continue to exist for a period of time in two forms: (1) in Reach More Parents' database backups for a period of no longer than 35 days from the date data is deleted; and (2) in Reach More Parents' server logs for a period no longer than 90 days from when the data was logged

ISSUE: Responding to a data breach

RISK: GDPR non-compliance

MITIGATING ACTION: Low-level auditing software is run on all production systems to record potentially malicious actions that may take place. If Reach More Parents become aware of a security breach of users' Personal Data, Reach More Parents will notify affected users as required by applicable laws and may post a notice on the Services as required by applicable laws. Reach More run regular vulnerability scans on its systems.

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: 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: Personal information used in the Reach More Parents platform is always kept to a minimum and is only visible by staff elected by the school. Reach More Parents will not access this information unless it is deemed necessary to do so for the purposes of support and in any instance will only access this information with permission from the school. The actions of all Parent Hub users (staff and parents) are logged to ensure that an audit trail is available. Parent Hub also use internal monitoring and auditing of its employees who are able to access data within the Parent Hub system

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

