Moorland Federation

DPIA BROMCOM

May 2025 - 2026

Moorland Federation

Somerset Council | Support Services for Education

Data Protection Impact Assessment

Submitting controller details

Name of controller	Moorland Federation
Subject/title of DPIA	Bromcom
Name of DPO	SSE Schools DPO dposchools@somerset.gov.uk

Step 1: Identify the need for a DPIA

Explain broadly what the 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.
Example: Bromcom MIS is a cloud-based Management Information System designed for schools. It processes personal and sensitive data relating to pupils, staff, and parents to support school operations including attendance, safeguarding, assessments, and communications. A DPIA is required due to the volume of personal and special category data processed and the use of cloud hosting.

Step 2: Describe the processing

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 Notice (pupils and parents / workforce) for the school provides the legitimate basis of why the school collects data. Specifically, this relates to keeping children safe on the school site.
Data is collected from school systems and users, processed and stored securely on Bromcom's UK-based servers with appropriate access controls.

How will you collect, use, store and delete data?

Example:

Data will be collected from the following: Staff input, uploaded records, third-party integrations (e.g., other EdTech tools or Local Authorities and other educational settings).

What is the source of the data?

Example:

Data will be collected from the following: Staff input, uploaded records, third-party integrations (e.g., other EdTech tools or Local Authorities and other educational settings).

Will you be sharing data with anyone?

Examples:

Data may be shared under lawful grounds with third-party partners, statutory bodies, and integration services listed in Bromcom's privacy documentation. It can also be shared with other Local Authorities and educational settings on change of school by the student.

What types of processing identified as likely high risk are involved?

Example:

Includes special category data (e.g., SEN, safeguarding), accessed through controlled user permissions and audit trails.

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?

Example: Pupil data relates to the name of the child, date of birth, and class. Data also includes attendance and SEN, as well as ethnicity health and religion. Data for contacts relating to pupils such as parents will also be recorded.

Special Category data?

Examples:

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?
Example:

Daily operational use for all enrolled pupils and staff. Applies to all users of the MIS across the trust or school.

Access is limited to password protected accounts and users will have defined permissions, only accessing data relevant to their roles.

How long will you keep the data for?

Example:

Aligned to school retention schedules and statutory requirements.

How many individuals are affected (students, workforce, governors, volunteers)? And what is the geographical area covered?

Example:

The individuals affected are the children and families within the school community, and staff employed within the Federation.

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?

Example:

The school collects and processes personal data relating to its pupils/students in order to keep children safe and comply with statutory guidance (KCSIE, Working Together).

Through the Privacy Notices (Pupil/Workforce/Governor/Visitors), the school is committed to being transparent about how it collects and uses data and to meeting its data protection obligations.

How much control will they have?

Example:

Children and families will have limited control over the information recorded on Bromcom. They have the right of access to the records, but redactions may be made if the DSL considers that disclosure may meet the 'serious harm' exemption for educational data in the Data Protection Act 2018. If the data subject or their representative disputes any recorded information, the school will not alter the record but may add a note e.g. *the parent disputes that this incident occurred and has requested that the record is adjusted to reflect their concerns.*

Do they include children or other vulnerable groups?

Example:

The data relates to students including students under 18 years of age (children in law)

Are there prior concerns over this type of processing or security flaws?

Example:

The information is stored on a cloud based system and administrator access to Bromcom is controlled by password access. There are no known security flaws.
Further information regarding privacy settings can be found here
https://bromcom.com/privacy/

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?

What do you want to achieve?

Example:

Systematic and secure record keeping related to information management.

What is the intended effect on individuals?

Example:

The intended effect on individuals is to ensure that personal data is managed securely, accurately, and efficiently to support the day-to-day operations of the Federation. This includes providing timely and effective support for pupils, streamlining communication with parents/carers, improving attendance, and enabling data-informed decision-making across the school community.

What are the benefits of the processing – for you, and more broadly?

Example:

The school using Bromcom will realise the following benefits:

1. Increased accuracy in pupil records and reporting
2. More responsive and coordinated interventions for pupils needing support
3. Reduced administrative burden on staff, allowing more time for teaching and learning
4. Enhanced transparency and access to information for parents (where appropriate)
5. Improved data security through a robust, cloud-based system with strong access controls

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?
Example: • Governors have been consulted. • The view of the SSE DPO has also been engaged to ensure Data Protection Law compliance

Step 4: Assess 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 minimization? 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?
What is your lawful basis for processing? Example: The lawful basis for processing personal data is contained in the school's Privacy Notices specifically Article 6(1)(c) Legal Obligation to fulfil our obligations under the following legislation: • Health and Safety at Work Act • Keeping Children Safe in Education • Safeguarding Vulnerable Groups Act • Working together to Safeguard Children Guidelines (DfE) The lawful basis for processing Special Category data is Article 9(2)(b). **Does the processing actually achieve your purpose?** Example: The use of Bromcom MIS enables the school or trust to meet its objectives in managing pupil, staff, and operational data efficiently and securely. The platform centralises multiple functions such as attendance tracking, safeguarding reporting, communications, behaviour management, assessments, and statutory returns, all within a single secure system. **Is there another way to achieve the same outcome?** Example: Similar outcomes could be achieved using manual or disparate digital systems (e.g. spreadsheets, paper records, and multiple standalone applications). However, these approaches are significantly less efficient, more prone to error, and carry greater data protection risks due to fragmented data storage, inconsistent processes, and limited access controls.

How will you prevent function creep?

Example:

Function creep will be prevented by ensuring that the use of Bromcom MIS is limited strictly to the purposes outlined in the school's or trust's Data Protection Policy and Privacy Notices. Data will only be processed where there is a clear legal basis and educational need.

How will you ensure data quality and data minimization?

Example:

Data quality and minimisation will be maintained through a combination of technical controls, policy measures, and staff training.

What information will you give individuals?

Example:

The school privacy notice ensures that data subjects and their representatives (e.g. parents) are aware that safeguarding concerns and incidents will be recorded to comply with KCSIE.

How will you help to support their rights?

Example:

The school has a Subject Access Request procedure in place to ensure compliance with Data Protection Law. Other rights e.g. rectification or deletion will be considered where there may be a conflict with the legal responsibilities of the school.

What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Example:

The data on the system is owned by the school and monitored by authorised personnel only. There will be no international transfer.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm Remote, possible or probable	Severity of harm Minimal, significant or severe	Overall risk Low, medium or high
1. Unauthorised Access to Personal Data	Possible	Severe	Medium
2. Data Retention Beyond Legal Limits	Possible	Significant	Medium

3. Inaccurate or Outdated Data	Possible	Significant	Medium
4. System Misconfiguration or Human Error	Probable	Significant	Medium

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	Options to reduce or eliminate risk	Effect on risk Eliminated reduced accepted	Residual risk Low, medium, high	Measure approved Yes / No
1. Unauthorised Access to Personal Data	Example: Implement strict role-based access controls in Bromcom, with regular audits of user permissions and access logs. Ensure all staff receive training on data confidentiality.	Reduced	Low	Yes
2. Data Retention Beyond Legal Limits	Example: Apply automated data retention rules in line with the IRMS Toolkit. Conduct annual data reviews and deletions, and maintain clear retention policies.	Reduced	Low	Yes
3. Inaccurate or Outdated Data	Example: Provide staff training on accurate data entry, implement validation checks, and conduct termly data quality audits. Integrate with official data sources (e.g. DfE) where applicable.	Reduced	Low	Yes
4. System Misconfiguration or Human Error	Example: Provide administrator training and implement peer checks for system configuration. Use two-factor authentication and confirmation prompts	Reduced	Low	Yes

	before data is exported or shared.			

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	Executive Headteacher	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Federation Business Managers	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Amy Brittan, SSE DPO	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: • Proceeding with implementation, provided access controls, training, and retention policies are in place and regularly reviewed. • Ensuring that Privacy Notices are updated to reflect Bromcom as a data processor and the types of data shared. • Maintaining a log of configuration changes and reviewing data sharing arrangements with third parties integrated with Bromcom. • Scheduling periodic internal audits and DPIA reviews to ensure compliance and adapt to any future changes in data processing. With these mitigations, the processing is lawful, proportionate, and meets the necessary data protection standards.		
DPO advice accepted or overruled by:	Executive Headteacher	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	Federation Business Managers	If your decision departs from individuals' views, you must explain your reasons

Comments:		
This DPIA will kept under review by:	Federation Business Managers	The DPO should also review ongoing compliance with DPIA