Data Privacy Impact Assessment

Submitting controller details

Name of controller	Lyngford Park Primary School
Subject/title of DPIA	Bromcom implementation
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.

- Bromcom will be the Management Information System for the Trust, replacing Capita SIMS.
- The DPIA is required as the information about individuals will be disclosed to organisations or people who have not previously had routine access to the information.
- We need to complete the PIA because of the sensitivity of the data held. Some of the data held is classified as Special Category under the UK GDPR e.g. health and medical information, ethnicity.
- We also need to ensure that no personal data is irretrievably lost during the migration from SIMS to Bromcom, due to the ongoing legal hold on data destruction placed by the Independent Inquiry into Child Sexual Abuse and the likelihood of needing to preserve pupil and personnel data indefinitely https://www.iicsa.org.uk/key-documents/115/view/2018-07-25-guidance-note-retention-instructions-data-protection-requirements-version-2.pdf

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?*

Bromcom will be the system in which learner and workforce details are held to manage the school including personal records, health information, timetabling, attendance, assessment, SEN, interventions, behaviour logs and communications.

The Trust are **data controllers** for the personal data held on Bromcom. Bromcom are **data processors** for any data they may access during the course of support calls or technical interventions and the data held on their servers.

1. How is this data processed by Bromcom? / 2. For what purpose is this data processed by Bromcom?

Bromcom will hold and process the data of students/staff only for the purposes of education management. Bromcom will only store and process such data as is required to provide the service to the Trust. Bromcom does not store Bromcom Customer data outside of the European Economic Area (EEA) (as required by the Department for Education).

Teachers are the end users of the data, with all other aspects of the setup being automated. However, if there are support issues, the Bromcom Education support team would have temporary access to Trust personal data to assist with the issue being faced.

Data is routinely backed up and backups are held for 30 days before being overwritten.

3. Where is this data processed and stored (in the UK, EU, etc...)?

Bromcom hosts all of its cloud hosted MIS services on the Microsoft Azure Platform and these services are run exclusively from the UK North and UK South Azure Regions, therefore all data stored on the Bromcom MIS cloud hosted solution remains in the UK only.

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?*

- Student: Name(s), addresses, addresses, emails, contact numbers, emergency contacts, gender, date of birth, UPN, ULN, UCI, Admission Number, enrolment status / history, previous schools, ethnicity / ethnic background, religion, nationality, languages, English proficiency, medical & dietary information, disabilities, doctor information, SEN information, gifted & talented, FSM, transport, looked after, child protection, related documents, funding and allowances, behaviour, attendance, assessment, exams, exclusions, reports, learning aims, support & support documents. Safeguarding incidents is an optional extra.

- Staff: Name(s), gender, ethnicity, date of birth, staff code, NI number, salary information, disabilities, religion, vehicles, languages, medical conditions, dietary

needs, telephones, emails, addresses, emergency contacts, absences, contracts, qualifications, CPD, relevant documents, background checks, SCR fields.

- Parent/Carer: personal identifiers, contact details (including full postal address).
- The data updates instantly upon changes made by the school.
- Bromcom does not sell or otherwise transfer Trust personal data to other organisations for the purposes of advertising or marketing. All data provided by the Trust for the purposes of processing is the under the ownership of the Trust.

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)?*

- The data relates to children and staff within the Trust. They will have no control over the data. The children would likely not fully understand the nature of the data processing, as such this would be something their parents/guardians would be concerned with. Their parents would most likely expect us to use the data in this way.
- No prior concerns or security flaws have been notified or identified, though there have been some recent data breaches related to cloud-based school systems e.g. WisePay. We will ensure, as much as possible, that we receive up to date notifications from Bromcom about any breaches or outages.
- The actual processing of the data is not novel and has been done by many systems over the years. The change from the existing system (SIMS) is that the data is stored online.

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 purpose of this project is to improve management at the Trust. The intended effect on individuals is improving teaching and learning outcomes, and therefore improving life chances for the children in the school's care.
- The benefits of using the system are accuracy in processing personal data, increased access too systems for school staff at school and home, a reduction in manual working through automation, and better monitoring of students.

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?*

- It is not appropriate to do so - we process this data as to comply with our legal and statutory duties under the Education Act and related legislation. Pupils, parents and staff will be informed through an updated privacy notice.

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?*

- Lawful basis: The **lawful basis** for schools using Bromcom is: Article 6(1)(c) Legal Obligation for the collection of attendance and core data required by the LA and DfE, and obligations under the Education Act 2002 and the Children Act 1989. For the processing of special category data, the lawful basis is Article9(2)(b) exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law; and Article 9(2)(c) necessary to protect the vital interests of the data subject or of another natural person where the Data Subject is physically or legally incapable of giving consent.

- There are other ways to achieve the outcome, but not with the flexibility of school/home access, which will reduce the risk of data loss or disclosure.

- The privacy notices for the Trust will be updated to include the details of this company and parents will be informed of the changes through a note in the newsletter linking to the updated notice.

- To ensure Bromcom comply with their legal duties, we have engaged with them to clarify their data protection policies and read/reviewed the contractual information relating to data protection (page 68-77 of the contract).

- No international transfers are involved, though sub-processors for Bromcom may receive some data. If this is the case, Bromcom's privacy information states that this will be compliant with UK and EU/EEA practices

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**	**Severity of harm**	**Overall risk**
1. Data currently on SIMS is not migrated or preserved	Possible	Severe (non-compliance with legal obligations)	High
2. Linked systems (payment; email accounts) do not accurately transfer leading to disruption to services and possible missing data	Possible	Significant	High
3. Current school or home technology does not effectively support Bromcom e.g. browsers are out of date; older versions of software or operating systems installed	Possible	Significant	Medium
4. Staff working at home do not have up to date security on home devices	Probable	Significant	Medium
5. Server breach at Bromcom Education - someone hacking into servers and accessing data	Remote	Severe	Low
6. Member of staff accessing data on the platform in an insecure location - in a public place, with members of the public seeing the data	Possible	Minimal	Medium
7. Member of staff accessing data on the platform in an insecure location - in a public place, and leaving the device unattended (e.g., to go to bathroom)	Remote	Severe	Medium
8. Member of staff accessing data on the platform in an insecure location - at home, with members of the household having access to the device when unattended	Possible	Minimal	Medium
9. Member of staff printing data from the system and leaving unattended	Possible	Severe	Medium
10. Member of staff abusing data within system for personal purposes or gain	Remote	Severe	Medium
11. Staff login details getting into the hands of an unauthorised person	Remote	Severe	Medium
12. Staff retain access when no longer in post – privacy risk due to unauthorised persons	Possible	Minimal	Medium

accessing system (non-compliance with Principle 6 of UK GDPR –integrity and confidentiality)			
13. Data not available at critical times due to Bromcom maintenance or outage – privacy risk due to lack of access to data (non-compliance with Principle 6 of UK GDPR –integrity and confidentiality)	Possible	Significant	Medium
14. Excessive data is added to Bromcom (non-compliance with Principle 3 of UK GDPR – data minimisation)	Possible	Minimal	Low
15. Parent requesting access to their child's data held in Bromcom (non-compliance with UK GDPR Article 15: Right of access)	Possible	Minimal	Medium
16. Parent does not want their child's data added to Bromcom (non-compliance with UK GDPR Article 21: Right to object)	Remote	Minimal	Medium
17. School do not renew contract with Bromcom – privacy risk from data being retained (non-compliance with Principle 5 of UK GDPR – Storage limitation) 1.	Remote	Minimal	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**	**Residual risk**	**Measure approved**
1/2	Trust must map data held on SIMS to ensure there is a full picture of all the data and linked systems held on SIMS. 5 years' worth of data can be migrated from SIMS to Bromcom. All residual data must be preserved in a way that can still allow access e.g. in the event of a subject access request	Reduced if appropriate measures in place	Medium/High	Must be confirmed by Trust
3/4	Audit school systems to ensure that technical specifications will meet Bromcom's requirements. Provide staff with information about what browser/OS will support Bromcom	Reduced	Low	Yes
6/7/8	Include clause in staff acceptable use policy related to use of Bromcom at home and school. Update guidance in staff IT induction documentation to ensure staff expectations are clear. Provide staff with support to check home devices are up to date	Reduced Reduced	Low Low	Yes Yes
6/7/8	Periodic regular notices reminding staff of their obligations under the acceptable use policy via email.	Reduced	Low	Yes
9	Update data protection policy to include clause stating that data should only be printed if absolutely necessary, and if printed should be kept with a member of staff or locked away at all times.	Reduced	Medium	Yes
6/7/8/9/10	Update guidance in staff IT induction documentation to ensure staff know of the restrictions outlined above.	Reduced	Medium	Yes
10/11	Periodic notices reminding staff of	Reduced	Medium	Yes

	their obligations under the data protection policy via email.	Reduced	Low	Yes
12	Ensure there is a robust removal procedure for staff accounts when the leave the school/MAT			
13	Ensure that MAT is receiving updates from Bromcom on possible outages for maintenance or security issues and these are communicated to staff who may require access at essential times.	Reduced	Low	Yes
15/16	Ensure that privacy notice is updated Ensure that MAT can extract data from Bromcom for students in the event of a subject access request. Consider how MAT would explain that 'right to object' is balanced by MAT's requirement to use the tool	Reduced	Low	Yes
`17	If school/MAT do not renew Bromcom, ensure that data is transferred or preserved in line with the agreement in the contract.			

Step 7: Sign off and record outcomes

Item	**Name/position/date**	**Notes**
Measures approved by:	SLT staff member name	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	In-school data protection lead	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:

The Trust and DPO have assessed the technical security measures required to implement Bromcom, and have identified the key issues, particularly around data transfer from SIMS and staff use of the tool.

The main residual risks remain around:

- Data transfer – the Trust must map all the data currently held on SIMS and all the

linked systems e.g. email, data integrators (e.g. Wonde), payment systems. The Trust must ensure that as much data as possible is migrated to Bromcom – upon research, it appears that this is five years' worth of data. Remaining data must be preserved in a way that can allow access if required. This is essential to comply with the legal hold on pupil/personnel data placed by the Independent Inquiry into Child Sexual Abuse and the likely extension of data retention schedules. • Staff use of the tool – ensuring that staff have appropriate home security in place, ensuring that information is not accidentally disclosed, or that access remains when staff leave. The measures required to reduce these risks are around staff training and reminders. The MAT Data Protection Lead and DPO will liaise on staff reminders for specific and general issues and ensure that the data protection policy reflects staff responsibilities		
DPO advice accepted or overruled by:	SLT staff member name	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	In-school data protection lead	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	In-school data protection lead	The DPO should also review ongoing compliance with DPIA