Data Protection Impact Assessment (BlueSky)

Cloud computing is a method for delivering information technology (IT) services in which resources are retrieved from the Internet through web-based tools and applications, as opposed to a direct connection to a server at the school. Hurst Green Primary School operates BlueSky which is a cloud based system. As such Hurst Green Primary School 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.

Hurst Green Primary School recognises that moving to a cloud service provider has a number of implications. Hurst Green Primary School 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 school 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 UK GDPR is satisfied by the school. Hurst Green Primary School 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.

Contents

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? – BlueSky is a system used by schools to assist in the professional development, educational research and learning development of teachers. It allows schools to triangulate performance reviews, professional development and quality assurance processes. Progress is easily evaluated, while staff are engaged through a rich, ongoing professional dialogue.

The BlueSky platform is uniquely flexible, meaning schools and trusts can tailor the process and terminology to match the School/Trust's values and priorities. With BlueSky, all school staff can have their own personal development portfolio. Whether they are a qualified teacher, support staff, school business management or catering – everyone can use BlueSky to support their professional development throughout their career.

BlueSky functionality includes the following:

Performance Reviews – Tailored performance reviews to reflect the culture of the School/Trust. Senior management is able to work with staff to link objectives to school priorities.

Professional Learning – Enables the School/Trust to develop and grow its staff through professional development effectively measuring the impact of learning on objectives.

Quality Assurance – Enhances the quality assurance process in line with the School/Trust culture. It enables the School/Trust to triangulate professional learning, objectives and school priorities.

BlueSky Education performance management software is used by a number of Schools/Trusts. BlueSky dedicated features help Schools/Trusts implement consistent processes for teacher, support and operations staff appraisal, and aggregate information across schools to track performance, identify best practice and share expertise.

Hurst Green Primary School will undertake the following processes:

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

By opting for a cloud based solution the school aims to achieve the following:

1. Scaleability
2. Reliability
3. Resilience
4. Delivery at a potentially lower cost
5. Supports mobile access to data securely
6. Update of documents in real time
7. Good working practice, i.e. secure access to sensitive files
8. Effective CPD for staff

BlueSky cannot do anything with the school's data unless they have been instructed by the school. The schools Privacy Notice will be updated especially with reference to the storing of pupil and workforce data in the cloud.

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 Notices (pupil and workforce) for the school provides the lawful basis of why the school collects data (lawful basis for the use of BlueSky is Article 6, 1 (e) processing is necessary for the performance of a task carried out in the public interest). BlueSky is referenced in the respective Privacy Notices. The school acts as the data controller BlueSky as the data processor for data and other content uploaded to the BlueSky platform by users from Hurst Green Primary School.

How will you collect, use, store and delete data? – The information collected by BlueSky is available on the secure online platform. The information is retained according to the school's Data Retention Policy.

What is the source of the data? – Workforce information is collected as part of staff appraisals, performance management. It includes staff names and email addresses, and their targets for appraisal. It captures their reflections, their progress and evidence towards their targets, and the outcomes. It would potentially store any capability programmes.

Will you be sharing data with anyone? – Hurst Green Primary School workforce data in relation to performance management and appraisals is uploaded securely to the cloud.

Hurst Green Primary School agrees to maintain the security and integrity of the system by refraining from inappropriate sharing of data and maintaining system security at all times.

What types of processing identified as likely high risk are involved? – Transferring 'special category' data from the school to the cloud. Storage of personal and 'special category 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? – Workforce data relating to personal information (such as name, school address and contact details, employee or teacher number.

The lawful basis for the use of BlueSky is Article 6, 1 (e) processing is necessary for the performance of a task carried out in the public interest.

Special Category data? – Some of the personal data collected may fall under the UK GDPR special category data. This includes race; ethic origin; and health.

The lawful basis for collecting special category information relates to Article 9 2 (g) *processing is necessary for reasons of substantial public interest and is authorised by domestic law.*

How much data is collected and used and how often? – Personal data is collected for the purposes of performance management, target setting and appraisals.

How long will you keep the data for? – Consider the data retention period as outlined in the IRMS Information Management Toolkit for Schools.

Scope of data obtained? – How many individuals are affected (pupils, workforce)? And what is the geographical area covered? Data collected relates to the workforce.

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 school provides education to its students with staff delivering the National Curriculum

What is the nature of your relationship with the individuals? – Hurst Green Primary School collects and processes personal data relating to its pupils and employees to manage the parent/pupil and employment relationship.

Through the Privacy Notice (pupil/workforce) Hurst Green Primary School 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? – The setting of performance management targets and appraisals is done in collaboration with and in agreement with the member of staff and a member from the Senior Management Team. Once set this will be subject to an annual appraisal.

Do they include children or other vulnerable groups? – Some of the data may include special category data such as race/ethnic origin and the health of an individual. BlueSky provides the school with appropriate access controls to the data ensuring that these are not shared with any further third party.

Are there prior concerns over this type of processing or security flaws? – All data is stored and encrypted locally on the schools device any data transmitted to the server data is encrypted in transport using TLS 1.2 and AES 128 GCM.

Hurst Green Primary School 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: BlueSky take the security of School/Trust personal data

seriously and have technical and organisational measures to ensure a level of security appropriate to the risk.

BlueSky use a mixture of measures including utilising technology to combat cybersecurity, data management techniques, user access and management procedures, physical security and guidelines for personnel.

BlueSky measures are aimed at having the ability to: (1) ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, and (2) restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

The BlueSky virtual servers are hosted within an AWS datacentre which maintain industry standard levels of security. Staff supporting or developing the BlueSky software only have access permissions as required by their role. BlueSky do have CE certification and carry out annual penetration tests.

- **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 stored and encrypted locally on the schools device any data transmitted to the server data is encrypted in transport using TLS 1.2 and AES 128 GCM. Data is encrypted at rest using AES 256.

- **ISSUE:** Use of third party sub processors?
  RISK: Non-compliance with the requirements under UK GDPR
  MITIGATING ACTION: BlueSky work closely with third parties (for example payment service providers, technical business partners, advertising analytics providers, search engine information providers, logistics service providers and subcontractors who provide services and goods to BlueSky to enable them to fulfil their customer contracts).

If BlueSky receive information about the School/Trust from them, BlueSky will inform the School/Trust of this and the purposes for which they intend to use that information.

Any sub-contractors used to support the BlueSky service are subject to GDPR terms that are no less onerous than those between BlueSky and the client.

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage.
  MITIGATING ACTION: BlueSky environment is hosted by AWS within the UK region.

- **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: BlueSky environment is hosted by AWS within the UK region.

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: BlueSky use a mixture of measures including utilising technology to combat cybersecurity, data management techniques, user access and management procedures, physical security and guidelines for personnel.

  BlueSky measures are aimed at having the ability to: (1) ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, and (2) restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: BlueSky store School/Trust personal data in accordance with their data retention policy, which sets out the categories of information they hold as a business and specific retention periods for each such category. These retention periods take into consideration the requirements of data protection law, the requirements of

other laws to keep information for certain minimum periods, the limitation periods for legal action and good industry practice.

The period for which BlueSky may keep personal data in line with their data retention policy will depend on the nature of School/Trust interactions with them.

The School/Trust will need to ensure that this supports the School/Trust Data Retention Policy.

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: If BlueSky learns of a suspected or actual personal data breach, the Data Protection Officer will need to perform an internal investigation and take appropriate remedial measures in a timely manner, according to the appropriate policy. Where there is any risk to the rights and freedoms of data subjects, BlueSky will need to notify the relevant data protection authorities without undue delay and, when possible, within 72 hours.

  All BlueSky employees are made aware of the data breach procedure.

- **ISSUE:** Data is not backed up
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The BlueSky environment is hosted within the UK region across two availability zones. Backups are taken daily and rotated on a 35 day cycle. The time to restore from an outage would depend on the severity of the outage, a full database restore will take approximately 2 hours. Servers can be created from images in a matter of minutes. The backups are overwritten on a 35 day cycle.

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: BlueSky environment is hosted by AWS within the UK region.

- **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: BlueSky comply with the data subject's rights under data protection law, in that under certain circumstances the data subject can:

Request access to your personal data.
Request correction of your personal data.
Request erasure of your personal data.
Object to processing of your personal data.
Request restriction of processing your personal data.
Request transfer or your personal data.
Right to withdraw consent.

In most cases the school will be able to provide the information requested as the data controller.

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The school as data controller maintains ownership of the data. Edulink One is the data processor. This relationship is documented in the Overnet Data Privacy Notice.

- **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: This should be monitored to address any changes in technology and its impact on data. The school should maintain ownership of the Cloud technologies used ensuring the current and future technologies enable UK GDPR compliance.

- **ISSUE:** UK GDPR Training
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Appropriate training is undertaken by personnel that have access to BlueSky within the school.
  All BlueSky staff undergo annual GDPR and Cyber Security training. BlueSky do not undertake DBS checks as none of their staff work with children or vulnerable adults.

  Only staff that require access to the BlueSky Education software are granted access appropriate with their role and only after a period of training.

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: AWS computing environments are continuously audited, with certifications from accreditation bodies across the world, including ISO 27001, FedRAMP, DoD CSM, and PCI DSS.

  All data is stored and hosted on AWS who hold the following certifications:

  ISO 27001: is one of the most widely recognized, internationally accepted independent security standards. AWS has earned ISO 27001 certification for the systems, applications, people, technology, processes, and data centres that make up its shared Common Infrastructure

  ISO 27017: is an international standard of practice for information security controls based on ISO/IEC 27002, specifically for Cloud Services. AWS has been certified compliant with ISO 27017 for its shared Common Infrastructure

  ISO 27018: is an international standard of practice for protection of personally identifiable information (PII) in Public Cloud Services. AWS has been certified compliant with ISO 27018 for its shared Common Infrastructure

  AWS is also fully compliant with applicable EU Data Protection laws, and the AWS Data Processing Agreement incorporates the Article 29 Working Party Model Clauses.

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:

- Scaleability
- Reliability
- Resilience
- Delivery at a potentially lower cost
- Supports mobile access to data securely

- Update of documents in real time
- Good working practice, i.e. secure access to sensitive files
- Effective CPD for staff
- Improve Teaching and Learning
- Succession planning, building future leaders

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: 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 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)
- Keeping Children Safe in Education 2018

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 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 identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no
Data Transfer	Secure network, end to end encryption	Reduced	Medium	Yes
Asset protection & resilience	Data Centre in UK, meets ISO 27001 standard	Reduced	Medium	Yes
Data Breaches	Documented in contract and owned by school	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:	Headteacher	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Headteacher	If accepting any residual high risk, consult the 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:

(1) Do any staff employed by BlueSky receive training in regard to data protection, linked to their duty of confidentiality or have DBS clearance? Is access to customer data granted on a role / permissions-basis?

[BlueSky] All staff undergo annual GDPR and Cyber Security training. We do not undertake DBS checks as none of our staff work with children or vulnerable adults. Only staff that require access to the BlueSky Education software are granted access appropriate with their role and only after a period of training.

(2) Are all BlueSky employees aware of the company data breach procedure?

[BlueSky] Yes, all employees are made aware of the data breach procedure

(3) Does BlueSky subcontract or not? And if so, do they meet the same standards of data protection / GDPR as yourselves?

[BlueSky] Any sub-contractors used to support the BlueSky service are subject to GDPR terms that are no less onerous than those between BlueSky and the client

(4) Is data encrypted between the school and the BlueSky server. If you use SSL encryption, could you advise what standard it meets (e.g. TLS 1.2 / AES-256bit)?

[BlueSky] data is encrypted in transport using TLS 1.2 and AES 128 GCM

(5) Where is the server located which hosts data from the school? (i.e. the UK)?

[BlueSky] Our environment is hosted by AWS within the UK region

(6) What service ISO certifications for the hosting of data (i.e. do you as a company hold ISO 27001 or is it the hosting company that holds the certification)?

[BlueSky] We don't hold ISO 27001 certification, however AWS is ISO 27001 certified

(7) What physical access controls exist, security of the servers, permission-based access, CCTV recording, Cyber Essentials certification, vulnerability and penetration testing.

[BlueSky] The BlueSky virtual servers are hosted within an AWS datacentre which maintain industry standard levels of security. Staff supporting or developing the BlueSky software only have access permissions as required by their role. We do have CE certification renewal November 2025 and carry out annual penetration test, next test by July 2025

(8) Should demand unexpectedly increase, can your server hosting service scale their facilities to meet demand?

[BlueSky] The BlueSky environment employs both Auto-healing to automatically replace a failing server and auto-scaling to increase capacity if the load increases beyond a threshold.

(9) What resiliency does the server hosting service provide for the availability of data? E.g. mirrored data centres, how often are backups taken and how long would it take to restore from an outage? Does the service manage all security updates for the service?

[BlueSky] The BlueSky environment is hosted within the UK region across two availability zones. Backups are taken daily and rotated on a 35 day cycle. The time to restore from an outage would depend on the severity of the outage, a full database restore will take approximately 2 hours. Servers can be created from images in a matter of minutes

(10) Is the BlueSky data encrypted at rest on the hosting servers?

[BlueSky] yes using AES 256

(11) Where the school may have deleted data and BlueSky holds the data on a backup, how long would it take for that data to be deleted from the backup? i.e. what is the backup rotation period if backups are overwritten?

[BlueSky] the backups are overwritten on a 35 day cycle

DPO advice accepted or overruled by: Accepted		
Comments:		
Consultation responses reviewed by: Headteacher If your decision departs from individuals' views, you must explain your reasons		
Comments:		
This DPIA will kept under review by:	School Business Manager	The DPO should also review ongoing compliance with DPIA