Data Protection Impact Assessment (IRIS Connect)

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. **Hales Valley Trust** operates IRIS Connect which is a cloud based system. As such **Hales Valley Trust** 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.

Hales Valley Trust recognises that moving to a cloud service provider has a number of implications. **Hales Valley Trust** 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 GDPR is satisfied by the school.

Hales Valley Trust 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? – IRIS Connect is a system used by schools to assist in the professional development, educational research and learning development of teachers. It provides an evidence based approach using video to assist teachers in the classroom setting in school.

IRIS Connect enables the teacher to record lessons, quickly and easily, using a mobile camera system (using iPads). After the recording has taken place, the video is uploaded directly to the teachers personal password account on the IRIS Connect online platform where the teacher can then watch it back as part of personal reflection and share with a colleague for feedback. IRIS Connect uses wireless audio technology with micro phones located around the classroom and the teacher wearing a wireless microphone. The recording will pick up images and audio of children commenting.

Hales Valley Trust 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 personal data
8. Effective CPD for staff.

IRIS Connect 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 legitimate basis of why the school collects data. IRIS Connect is referenced in the respective Privacy Notices. The school acts as the data controller and IRIS Connect as the data processor for videos and other content uploaded to the IRIS Connect platform by users from **Hales valley Trust**

How will you collect, use, store and delete data? – The information collected by IRIS Connect 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? – Pupil images and audio is collected within the classroom by virtue of the video recording.

Workforce information (the teacher leading in the classroom setting) is collected via images and audios.

Hales Valley Trust aims to ensure that (1) The recording equipment is positioned such that it's visible, safely located and unlikely to record sensitive or inappropriate content; (2) that all uploaded content is appropriate, non intrusive and aligned with the purpose; (3) when recording to remind those around you that the IRIS Connect camera is present in the room and the purpose of recording video and audio and (4) to exclusively use the system in a way which is aligned with the purpose.

Will you be sharing data with anyone? – **Hales Valley Trust** images and videos of pupils and teachers are uploaded securely to the cloud. For the purposes of assessment and evaluation the images and audio may be shared with a third party as part of an assessment.

Hales Valley Trust 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? – Pupil data relating to personal identifiers and contacts (such as name, unique pupil number, contact details and address) will not be used. The video and audio recording may pick up the following characteristics such as ethnicity, language, nationality, and gender.

Workforce data relating to personal information (such as name, address and contact details, employee or teacher number, bank details, national insurance number, marital status, next of kin, dependents and emergency contacts) will not be used. Special categories of data (such as gender, age, ethnic group) may be picked up.

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

How much data is collected and used and how often? – Personal data is collected for all pupils within the classroom setting when video recording. Additionally personal data is also held respecting the school's workforce (teaching staff/teaching assistants in the classroom setting).

How long will you keep the data for? – Consider the data retention period as outlined in **Hales Valley Trust** Retention Policy.

Scope of data obtained? – How many individuals are affected (pupils, workforce)? And what is the geographical area covered? EYFS to Year 6 pupils **630** and workforce **90.**

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? – **Hales Valley Trust** 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) **Hales Valley Trust** 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 IRIS Connect system is based on individual user accounts and permissioning. This means that the observed user has to agree to a recording taking place before the system allows another user to connect to the camera.

The same protection exist once a video has been encrypted and uploaded. This means that users are only able to see data that has been explicitly shared with them. By default users are limited to sharing videos with other users at their organization, although collaboration with other organisations can be enabled at the request of the clients Organisation Administrator.

Users have complete control over who has access to their data by deciding to share observations either with individual users or in a group library. Users will never "lose sight or control" of their video. Users will always be able to see their video and associated data. Users retain the right to delete a video or remove sharing privileges at any time.

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. IRIS Connect provides the school with appropriate access controls to the videos ensuring that these are not shared with any further third party. For example, files designated as private – only you can access the files; public – everyone can view the files without any restriction; and shared – only people you invite can view the files.

Are there prior concerns over this type of processing or security flaws? – All data is secured in transit using SSL encryption. It is securely restored at rest within industry leading data storage standards.
Hales valley Trust 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: Managed by a web platform designed to meet and, wherever possible, exceed security obligations

- **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 secured in transit using SSL encryption. It is securely restored at rest within industry leading data storage standards

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: Data is stored within an environment which utilizes state of the art network security, electronic surveillance, physical security and multi factor access control systems along to protect client data. The data centres are staffed 24 X 7 by trained security teams. Within their Privacy Notice IRIS Connect confirm that any sub processors they use to host the school's data meet GDPR and that they have relevant sub-processor agreements in place

- **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: The servers are based in Dublin, Ireland

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: GDPR non-compliance
  MITIGATING ACTION: Security systems are regularly updated and reviewed by an inhouse team of engineers with the advice of industry leading consultants and are subjected to regular 3rd party penetration testing. Staff are restricted from accessing client data by multiple levels of technical and procedural security

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: GDPR non-compliance
  MITIGATING ACTION: The End User Licence Agreement gives the school the right to delete videos and ensures that individual videos will not be recorded or shared with any other IRIS Connect user without the school's explicit consent

- **ISSUE:** Responding to a data breach
  RISK: GDPR non-compliance
  MITIGATING ACTION: If IRIS Connect learns of a suspected or actual personal data breach, the Data Protection Officer will perform an internal investigation and take appropriate remedial measures in a timely manner, according to the Data Breach

Policy. Where there is any risk to the rights and freedoms of data subjects, the IRIS Connect will notify the relevant data protection authorities without undue delay and, when possible, within 72 hours

- **ISSUE:** No deal Brexit
  RISK: GDPR non-compliance
  MITIGATING ACTION: IRIS Connect will continue to operate within all data protection laws for the UK in the eventuality of a no deal Brexit. IRIS Connect data is currently held in Ireland but the service they use also has a data centre in England, meaning IRIS Connect could easily move the data if necessary

- **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: As the data processor, IRIS Connect would not respond directly to a SAR. The school, as data controller, would decide if the SAR was appropriate and then contact IRIS Connect with the data they wish to provide to the data subject. IRIS Connect would be able to make all necessary information available to the school (such as enabling downloading of videos), at the request of the school

- **ISSUE:** Data Ownership
  RISK: GDPR non-compliance
  MITIGATING ACTION: Each IRIS Connect client nominates an Organisation Administrator who is responsible for agreeing to and enforcing the IRIS Connect End User Licence Agreement (EULA) when the school first signs into the system. The copyright of material generated by the school remains the property of the school. The school also has the right to decide which videos get uploaded to the system and, in day to day use, to decide how long they are stored for, when they are deleted and who has access to them

- **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 GDPR compliance

- **ISSUE:** Security of Privacy
  RISK: GDPR non-compliance
  MITIGATING ACTION: The cloud provided has the following assurances: ISO 27001 (widely adopted security standard); ISO 9001 (global standard for managing the quality of products and services); G Cloud; PCI DSS Level 1 (Payment Card Industry Data Standard); etc

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
No deal Brexit	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 EU, Certified, Penetration Testing and Audit	Reduced	Medium	Yes
Data Breaches	Documented in contract and owned by school	Reduced	Low	Yes
No deal Brexit	Moving data to hosted servers in England	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:	**Chief Operations Officer**	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	**Chief Operations Officer**	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) Cloud solution and the geographical location of where the data is stored to determine which Privacy Law apply? (2) Subject Access Requests and the technical capability to retrieve data in a structured format to provide the information to the data subject? (3) No deal brexit		
DPO advice accepted or overruled by:	**Yes**	If overruled, you must explain your reasons
Comments: **[DPO Advice provided]**		
Consultation responses reviewed by:	**Chief Operations Officer**	If your decision departs from individuals' views, you must explain your reasons
Comments: **[Comments provided]**		
This DPIA will kept under review by:	**Your IG**	The DPO should also review ongoing compliance with DPIA