Data Protection Impact Assessment (Google Classroom)

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 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? – Google Classroom is an online platform that both teachers and students can access. Google Classroom aims to simplify creating, distributing, and grading assignments in a paperless way. Its primary purpose is to streamline the process of sharing files between teachers and students. As such it delivers a cost effective solution to meet the needs of the business. In this setting access to Google Classroom is via RM Unify which in this instance is a Single Sign On means to access the Google Classroom environment (schools log into RMUnify- select the GSuite tile - land on the users GSuite page). **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 sensitive files Google Classroom has the ability to link with Google Drive, Google Docs, Sheets and Slides, and Gmail together to help the school achieve a paperless system. The school can invite students to classrooms through the school's ICT infrastructure, through a private code that can then be added in the student's user interface or automatically imported from a school domain.

Each class created with Google Classroom creates a separate folder in the respective user's Google Drive, where the student can submit work to be graded by a teacher.

Assignments can be stored and graded on Google's suite of productivity applications that allow collaboration between the teacher and the student or student to student. Instead of sharing documents that reside on the student's Google Drive with the teacher, files are hosted on the student's Drive and then submitted for grading. Teachers may choose a file that can then be treated as a template so that every student can edit their own copy and then turn back in for a grade instead of allowing all students to view, copy, or edit the same document. Students can also choose to attach additional documents from their Drive to the assignment.

- Google Classroom supports many different grading schemes. Teachers have the option to attach files to the assignment which students can view, edit, or get an individual copy.
- Students can create files and then attach them to the assignment if a copy of a file wasn't created by the teacher.
- Teachers have the option to monitor the progress of each student on the assignment where they can make comments and edit.
- Turned in assignments can be graded by the teacher and returned with comments to allow the student to revise the assignment and turn back in.
- Once graded, assignments can only be edited by the teacher unless the teacher turns the assignment back in.

The information is held securely with regular data backed up. The network is only accessible through dedicated password linked to the school.

Cloud based systems enable the school to upload documents, photos, videos, and other files to a website to share with others or to act as a backup copy. These files can then be accessed from any location or any type of device (laptop, mobile phone, tablet, etc).

The cloud service provider 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. **How will you collect, use, store and delete data?** – The information collected by the school is retained on the school's computer systems and in paper files. 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. Pupil information also includes classroom work, assessments and reports. Workforce information is collected through application forms, CVs or resumes; information obtained from identity documents, forms completed at the start of employment, correspondence, interviews, meetings and assessments. **Will you be sharing data with anyone?** – Hales Valley Trust 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 Integris and various third party Information Society Services applications. **Hales Valley Trust** routinely shares workforce information internally with people responsible for HR and recruitment (including payroll), senior staff, with the Local Authority, and the Department for Education. **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. However, in terms of using Google Classroom no special category data will be used.

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, unique pupil number, contact details and address). Characteristics (such as ethnicity, language, nationality, gender, religion, data of birth, country of birth, free school meal eligibility). Special education needs, safeguarding information, medical and administration (doctors information, child health, dental health, allergies, medication and dietary requirements). Attendance information, assessment, attainment and behavioral information. The school also obtains data on parents/guardians/carers including their name, address, telephone number and e-mail address. Workforce data relates 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). Special categories of data (such as gender, age, ethnic group). Contract information (such as start dates, terms and conditions of employment, hours worked, post, roles and salary information, pensions, nationality and entitlement to work in the UK). Work absence information, information about criminal records, details of any disciplinary or grievance procedures. Assessments of performance (such as appraisals, performance reviews, ratings, performance improvement plans and related correspondence). Information about medical or health conditions. **Special Category data?** – Some of the personal data collected falls under the GDPR special category data. This includes race; ethic origin; religion; biometrics; and health. These may be contained in the Single Central Record, RM Integris, child safeguarding files, SEN reports, etc. However, in terms of using Google Classroom no special category data will be used. **How much data is collected and used and how often?** – Personal data is collected for all pupils. Additionally personal data is also held respecting the school's workforce, Board of Governors, Volunteers, and Contractors. Data relating to sports coaches and other educational specialist is contained within the Single Central Record to ensure health and safety and safeguarding within the school. **How long will you keep the data for?** – The school will be applying appropriate data retention periods as outlined in its Data Retention Policy and the IRMS Information Management Toolkit for Schools. **Scope of data obtained?** – Google Classroom relies on minimal personal data. The school will act as the administrator and will set up access to pupils within a classroom and

individual setting. Personal data will include details of the class/year and the first and second name of the pupil.

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? – Access to the pupil files will be controlled by the school. The pupil will be able to login to RM Unify and get access to the classroom domain..

The teacher can set up individual user accounts enabling pupils to receive assignments and have them marked. Each account will have the class/year of the pupil and their first and last name.

Cloud Service provider is hosting the data and will not be accessing it.

The school will be able to upload personal data from its PC for the data to be stored remotely by a service provider. Any changes made to files are automatically copied across and immediately accessible from other devices the school may have.

Do they include children or other vulnerable groups? – None of data used in Google Classroom will have special category data such as child safeguarding records, RM Integris, SEN records, Single Central Record.

Are there prior concerns over this type of processing or security flaws? – Does the cloud provider store the information in an encrypted format? What is the method of file transfer? For example, the most secure way to transfer is to encrypt the data before it leaves the computer. Encryption does have its limitations inasmuch as the encryption key will need to be shared with others to access the data.

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: Google data centers are built with custom-designed servers, running Google's own operating system for security and performance. Google has 700+ security engineers that work around the clock to spot threats early and respond quickly

  Google's data centers use custom hardware running a custom hardened operating system and file system. Each of these systems has been optimized for security and performance. Google controls the entire hardware stack and is able to quickly respond to threats or weaknesses that may emerge

  Google is the first major cloud provider to enable Perfect Forward Secrecy, which encrypts content as it moves between Google servers and those of other companies

  Google encrypts Gmail, Attachment, and Drive data while in transit. This ensures that messages are safe not only when they move between the school and Google's servers, but also as they move between Google's data centers

- **ISSUE**: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred
  MITIGATING ACTION: Data is encrypted at several levels. Google forces HTTPS (Hypertext Transfer Protocol Secure) for all transmissions between users and GSuite

services and uses Perfect Forward Secrecy (PFS) for all its services. Google also encrypts message transmissions with other mail servers using 256-bit Transport Layer Security (TLS) and utilizes 2048 RSA encryption keys for the validation and key exchange phases. This protects message communications when client users send and receive emails with external parties also using TLS

PFS requires that the private keys for a connection are not kept in persistent storage. Anyone who breaks a single key can no longer decrypt months' worth of connections; in fact, not even the server operator is able to retroactively decrypt HTTPS sessions.

- **ISSUE**: Security of data whilst hosted in the cloud
  RISK: Risk of compromise and unlawful access when personal data is at rest
  MITIGATING ACTION: Customer data that is uploaded or created in GSuite services is encrypted at rest. Google have also enabled HTTPS for all of its GSuite services, including Google Classroom, so that the school data is encrypted when traveling from a school device to Google and also while in transit between Google data centers

  All Google employees are required to sign a confidentiality agreement and complete mandatory confidentiality and privacy trainings, as well as a Code of Conduct training. Google's Code of Conduct specifically addresses responsibilities and expected behaviour with respect to the protection of information
- **ISSUE:** Use of third party sub processors?
  RISK: Non compliance with the requirements under GDPR
  MITIGATING ACTION: Google Group companies directly conduct the majority of data processing activities required to provide the GSuite and Google Cloud Platform services. However, Google do engage some third-party processors to assist in supporting theseservices

  Each data processor goes through a rigorous selection process to ensure it has the required technical expertiseand can deliver the appropriate level of security and privacy. Google make information available about Google groupsub processors supporting GSuite and Google Cloud Platform services, as well as third-party sub processors involved in those services, and Google include commitments relating to sub processors in current and updated data processing agreements**ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: School data is protected as if it were on its own server. Unauthorized parties cannot access school data. Other customers cannot access school data, and the school cannot access theirs. All user accounts are protected by Google's secure architecture that ensures that one user cannot see another user's data

- **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: Google Cloud Platform (GCP) allows customers to choose to store their data in Europe, North America, or Asia. If applicable the school would specify this location when they configure their application to ensure compliance under GDPR

  Google's certification under the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks includes GSuite and Google Cloud Platform. Google have also gained confirmation of compliance from European Data Protection Authorities for its model contract clauses, affirming that Google's current contractual commitments for GSuite and Google Cloud Platform fully meet the requirements under GDPR in terms of transfers of personal data from the EU to the rest of the world

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: GDPR non-compliance
  MITIGATING ACTION: Google provides capabilities and contractual commitments created to meet data protection recommendations provided by the Article 29 Working Party. Google offers to sign EU Model Contract Clauses and a Data Processing Amendment for GSuite and Data Processing Amendments for Google Cloud Platform

  GDPR restricts the movement of data from the EU to non-EU countries that do not meet the EU's "adequacy" standard for privacy protection. Processing personal data strictly within the EU is a means of compliance with this regulation

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: GDPR non-compliance
  MITIGATING ACTION: Google provide tools to make it easy for the school to take its data without penalty or additional cost imposed by Google. Administrators can export customer data in standard formats at any time during the term of any agreement entered into by the school and Google. Google Cloud Platform customers can extract their data using industry standard tools, for which there may be charges.

- **ISSUE:** Responding to a data breach
  RISK: GDPR non-compliance
  MITIGATING ACTION: GSuite and Google Cloud Platform provide contractual commitments around incident notification for many years. Google will continue to

promptly inform schools of incidents involving its data in line with the data incident terms in Google's current agreements and the updated terms that apply when the GDPR came into force

Google's security practices are verified and certified by third-party auditors. Google has achieved ISO 27001 certification, which means that an independent auditor has examined the controls present in its data centers, infrastructure, and operation

Amongst these practices, employees are subject to background investigations based on their level of access. Any employee access is governed by a policy of "least privilege access," which means that access is only granted to the information and resources that are necessary for the execution of the assigned task

- **ISSUE:** No deal Brexit
  RISK: GDPR non-compliance
  MITIGATING ACTION: Google Cloud Platform (GCP) allows customers to choose to store their data in Europe, North America, or Asia. If applicable the school would specify this location when they configure their application to ensure compliance under GDPR
- **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: Data controllers can use the GSuite and Google Cloud Platform administrative consoles and services functionality to help access, rectify, restrict the processing of, or delete any data that they and their users put into Google systems. This functionality will help the school fulfill its obligations to respond to requests from data subjects when exercising their rights under the GDPR

- **ISSUE:** Data Ownership
  RISK: GDPR non-compliance
  MITIGATING ACTION: The school as data controller retains ownership of the data. Google Classroom is the data processor

- **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: Google's application and network architecture is designed for maximum reliability and uptime. Data is distributed across Google's servers and data centers. If a machine—or even an entire data center—fails, school data will still be accessible. Google owns and operates data centers around the world to keep the

services the school uses running 24 hours a day, 7 days a week

Google's application and network architecture is designed for maximum reliability and uptime. Google's computing platform assumes ongoing hardware failure, and it uses robust software failover to withstand disruption.

All Google systems are inherently redundant by design, and each subsystem is not dependent on any particular physical or logical server for ongoing operation. Data is replicated multiple times across Google's clustered active servers so that, in the case of a machine failure, data will still be accessible through another system.

Google also replicate data to secondary data centers to ensure protection from data center failures

- **ISSUE:** Security of Privacy
  RISK: GDPR non-compliance
  MITIGATING ACTION: Google is subject to independent verification of its security, privacy, and compliance controls. In order to provide this, Google undergo several independent third-party audits on a regular basis

  For each one, an independent auditor examines Google's data centers, infrastructure, and operations

  ISO 27001: is one of the most widely recognized, internationally accepted independent security standards. Google has earned ISO 27001 certification for the systems, applications, people, technology, processes, and data centers that make up its shared Common Infrastructure as well as for GSuite and Google Cloud Platform

  ISO 27017: is an international standard of practice for information security controls based on ISO/IEC 27002, specifically for Cloud Services. Google has been certified compliant with ISO 27017 for GSuite and Google Cloud Platform

  ISO 27018: is an international standard of practice for protection of personally identifiable information (PII) in Public Cloud Services. Google has been certified compliant with ISO 27018 for GSuite and Google Cloud Platform

  The American Institute of Certified Public Accountants (AICPA) SOC 2 (Service Organization Controls) and SOC 3 audit framework defines Trust Principles and criteria for security, availability, processing integrity, and confidentiality. Google

has both SOC 2 and SOC 3 reports for Google Cloud Platform and GSuite

This means that independent auditors have examined the controls protecting the data in Google's systems (including logical security, privacy, and data center security), and assured that these controls are in place and operating effectively

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

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)

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	Where applicable documented in contract and owned by school	Reduced	Low	Yes
No deal Brexit	Contingency plans in place	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: **[DPO Advice provided]**		
DPO advice accepted or overruled by:	**Yes**	If overruled, you must explain your reasons
Comments: **[DPO Advice provided]**		
Consultation responses reviewed by:	**Rachel Evans**	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