Data Protection Impact Assessment (Zoom)

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. Summerhill School operates a cloud based system. As such Summerhill 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.

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

Summerhill 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.

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? – The Zoom app allows schools to communicate with staff, School Governors, parents, students and other key stakeholders. The Zoom app enables schools to: (1) Engage with others from anywhere. (2) Meet from anywhere with any number (up to 100 attendees). (3) Call from anywhere. (4) Collaborate from anywhere. The use of Zoom will help the school to deliver a cost effective solution to meet the needs of the business. The popularity of Zoom rapidly increased during the Covid-19 Pandemic. Zoom was originally built for business customers, with privacy settings commensurate with commercial usage. However, it has become one of the main ways that individuals have sought to connect with each other, for work, education and social purposes. Core features include virtual video break out rooms and live whiteboard sharing, video chat, webinars for up to 100 interactive attendees and group messaging. Zoom has attracted much negative press attention over its Cyber-security and for its privacy settings. The most obvious, and widely reported risk, associated with Zoom is the potential for uninvited guests to access a meeting, referred to as 'Zoom Bombing'. Despite this, the UK Government chose to use Zoom to conduct meetings and publicised this. Many schools have taken this as an assurance that if it is suitable for the UK Government then it is suitable for schools. Zoom have acknowledged the concerns around the use of their platform and set out the steps they are taking to address concerns in a blog post and published guidance for administrators on setting up and securing a virtual classroom. Schools have been made aware of high profile security breaches on Zoom which has been the result of data being wrongfully shared by users. In this scenario the details, date and time of the meeting was shared freely over Twitter and wasn't password protected. Schools recognise the need to maintain the same high standards of data protection, when sharing events and lessons via video conferencing, as they would sharing any other sensitive, personal or confidential data.

Summerhill 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

The school can easily upload data to the cloud. The information can be accessed from any location and from 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 also stored in the cloud. 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? – Summerhill School 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, and various third party Information Society Services applications.

Summerhill School 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 Zoom the use of special category data will be limited to the lawful basis as outlined in the school's Privacy Notice (Student).

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. In terms of using Zoom special category data may be discussed. Whatever special category data is used the school will ensure that it has a lawful basis to do this and that this is documented in the school's Privacy Notice (Pupil). **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? – How many individuals are affected (pupils, workforce, governors, volunteers)? And what is the geographical area covered? Reception, Year 1 to Year 6 pupils. Zoom will be used by the school for the purposes of communication. The school will act in accordance with the lawful basis it has for using personal data. This is outlined in the schools Privacy Notice (Pupil) and Privacy Notice (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?** – Summerhill School collects and processes personal data relating to its pupils and employees to manage the parent/pupil and employment relationship. Through the Privacy Notice (student/workforce) Summerhill 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?** – Access to the files will be controlled by username and password. 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?** – In terms of using Zoom special category data may be shared verbally, for example, to provide an update on safeguarding concerns respecting a pupil(s). Whatever special category data is used the school will ensure that it has a lawful basis to do this and that this is documented in the school's Privacy Notice (Student).

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.

Summerhill 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: Zoom is committed to protecting the school's personal data. Zoom use a combination of industry-standard security technologies, procedures, and organizational controls and measures to protect school data from unauthorized access, use, or disclosure

- **ISSUE**: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred
  MITIGATING ACTION: The encryption that Zoom uses to protect meetings is TLS. This is different from end-to-end encryption because the Zoom service itself can access the unencrypted video and audio content of Zoom meetings. This may have some bearing on what is discussed and recorded when the school uses Zoom.

  However, it would appear that end to end encryption may be available to fee paying customers which would provide the school with a mitigating control, i.e. the free version of Zoom has a higher level of risk

- **ISSUE:** Use of third party sub processors?
  RISK: Non compliance with the requirements under GDPR
  MITIGATING ACTION: A subprocessor is a third party data processor engaged by Zoom, who has or potentially will have access to or process customer data. Prior to engaging any third party subprocessor, Zoom undertakes a due diligence test to evaluate the sub processors security and privacy posture

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: Zoom Video Communication, Inc. participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield. Zoom is committed to subjecting all personal data received from EU

member countries, Switzerland, and the United Kingdom, in reliance on the Privacy Shield Frameworks, to the Framework's applicable Principles

The European Court of Justice (ECJ) has ruled that the EU-US Privacy Shield is invalid as it fails to protect privacy and data protection rules. As part of the same ruling the ECJ decided that another data transfer mechanism, Standards Contractual Clauses, or SCCs, remain valid. The school will need to confirm whether an SCC is 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: Zoom services generally store data in the United States, though through its global data centers, data may come in from wherever users are located. Data may be transferred to the U.S., or to third parties acting on Zoom's behalf, for the purposes of processing or storage. Zoom may store local data locally in order to comply with specific local laws and regulations. By using Zoom the school consents to the transfer and storage of personal data in the U.S

  Zoom Video Communication, Inc. participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield. Zoom is committed to subjecting all personal data received from EU member countries, Switzerland, and the United Kingdom, in reliance on the Privacy Shield Frameworks, to the Framework's applicable Principles

  Zoom is responsible for the processing of personal data it receives under the Privacy Shield Framework, and subsequently transfers to a third party acting as an agent on its behalf. Zoom complies with the Privacy Shield Principles for all onward transfers of personal data from the EU, Switzerland, and the United Kingdom including the onward transfer liability provisions.

  In certain cases, Zoom will transfer personal data from the EU in accordance with the European Commission-approved Standard Contractual Clauses

- **ISSUE:** Being transparent if and when meetings are recorded
  RISK: GDPR non-compliance
  MITIGATING ACTION: All recordings of meetings are accompanied by a notice that a recording is taking place. Zoom alerts participants via both audio and video when they join meetings if the school is recording a meeting, and participants have the option to leave the meeting

The notice also links to the schools Privacy Notice(s) for online participants, and the school, as data controller, controls which attendees have permission to record

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: GDPR non-compliance
  MITIGATING ACTION: When operating as a processor, Zoom makes available to schools, as data controllers, the personal data of its data subjects and the ability to fulfill data subject access requests when they exercise their rights under the GDPR. This is done in a manner consistent with the functionality of the product and Zoom's role as a processor

- **ISSUE:** Use of new technology that might be perceived as being privacy intrusive
  RISK: GDPR non-compliance
  MITIGATING ACTION: Potentially. The use of video conferencing within people's homes may be perceived by some as privacy intrusive. However, individuals are not compelled to join video calls or to join via video as it is possible to join via audio call only

- **ISSUE:** Is the use of new technology likely to raise privacy concerns around the discussion of special category data that an individual would consider private?
  RISK: GDPR non-compliance
  MITIGATING ACTIONS: The information collected may include data that relates to children who are identified under the GDPR as requiring extra safeguards to protect their data. The information that is shared with the processor is the name and email address of the person that is set up on the account

  If the content of the video conference is recorded, then this may be process by the processor. However, it remains the data controller's choice whether this recording is stored locally or is retained in the Zoom cloud

  Zoom have access controls to prevent unauthorized access to meeting recordings saved in the cloud

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: GDPR non-compliance
  MITIGATING ACTION: Zoom will retain personal data collected for as long as required to do what they as written in their Privacy Notice, unless a longer retention period is required by law. The school can delete their own content in accordance with their data retention policy

- **ISSUE:** Responding to a data breach
  RISK: GDPR non-compliance
  MITIGATING ACTION: Zoom Video Communication, Inc. participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield. Zoom is committed to subjecting all personal data received from EU member countries, Switzerland, and the United Kingdom, in reliance on the Privacy Shield Frameworks, to the Framework's applicable Principles

  The European Court of Justice (ECJ) has ruled that the EU-US Privacy Shield is invalid as it fails to protect privacy and data protection rules. As part of the same ruling the ECJ decided that another data transfer mechanism, Standards Contractual Clauses, or SCCs, remain valid. The school will need to confirm whether an SCC is in place.

- **ISSUE:** No deal Brexit.
  RISK: GDPR non-compliance.
  MITIGATING ACTION: Zoom is committed to subjecting all personal data received from EU member countries, Switzerland, and the United Kingdom, in reliance on the European Commission-approved Standard Contractual Clauses

- **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: When operating as a processor, Zoom makes available to schools, as data controllers, the personal data of its data subjects and the ability to fulfill data subject access requests when they exercise their rights under the GDPR. This is done in a manner consistent with the functionality of the product and Zoom's role as a processor

  To make a request, data subject access requestors can contact Zoom's Privacy Team at privacy@zoom.us

- **ISSUE:** Data Ownership
  RISK: GDPR non-compliance
  MITIGATING ACTION: Zoom is the data processor, processing the school's personal data through the use of Zoom. The school as data controller still has ownership of the data

- **ISSUE:** Security of Privacy
  RISK: GDPR non-compliance
  MITIGATING ACTION: Zoom Video Communication, Inc. participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield. Zoom is committed to subjecting all personal data received from EU

member countries, Switzerland, and the United Kingdom, in reliance on the Privacy Shield Frameworks, to the Framework's applicable Principles

The European Court of Justice (ECJ) has ruled that the EU-US Privacy Shield is invalid as it fails to protect privacy and data protection rules. As part of the same ruling the ECJ decided that another data transfer mechanism, Standards Contractual Clauses, or SCCs, remain valid. The school will need to confirm whether an SCC is in place.

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 (Student 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 by becoming a fee paying customer	Reduced	Medium	Yes
		Reduced	Medium	Yes
Asset protection & resilience	Data Centre in EU, Certified, Penetration Testing and Audit			
Data Breaches	Documented in Microsoft's Online Services Terms	Reduced	Low	Yes
No deal Brexit	Appropriate Standard Contract Clauses are applied	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:	Martyn Palfreyman	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Martyn Palfreyman	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: That Zoom is added to the school's Privacy Notices (Students, Workforce and Governors) Ensure the school apply robust technical and organizational privacy settings to safeguard privacy of Zoom participants Advise that the use of Zoom should be restricted as far as is possible. There are a number of issues that have been flagged, such as 'Zoom bombing' and using Zoom when there is an alternative provision available. Based on the DPIA the school have accepted the risks and wish to use Zoom Advise that the school becomes a fee paying customer which adds a level of integrity and confidentiality to the Zoom platform		
DPO advice accepted or overruled by:	**[Yes/No]**	If overruled, you must explain your reasons
Comments: **[DPO Advice provided]**		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments: **[Comments provided]**		
This DPIA will kept under review by:	Vicki Poole	The DPO should also review ongoing compliance with DPIA