Newbold and Tredington C of E Primary School and Day Nursery

Creating a chance to SHINE every day

Data Protection Impact Assessment (Teams)

The Data protection Impact Assessment is systematic process for identifying and addressing privacy issues and considers the future consequences for privacy of a current or proposed action.

Section 3 Article 35(1) states “Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in high risk to the rights and freedoms of natural persons, the controller shall, prior to processing, carry out an assessment of the impact of the envisaged processing operation on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.”

DPIA template for screening questions and completing an assessment

The following screening questions will identify if a DPIA is required. Answering ‘yes’ to any question will require a DPIA to be completed. You may expand on the answers as work progresses.

Initiative name: **Using Teams for Remote learning and homework**
Name and position of individual responsible of DPIA: **Samantha Welsby (Head)**
Assessment Date: **November 2020**

Number	Question	No	Yes	Comments
1	Will the initiative involve the collection of new information about individuals?	No		
2	Will the initiative compel individuals to provide information about themselves?		Yes	Children and staff will potentially be using video conferencing in their own homes.
3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? NB. This includes individuals who have previously accessed information but now work for a different organisation.	No		Potentially if the videos are shown to other people
4	Will you be using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?		Yes	Not normal use of teams meetings - normally adult only meetings

5	Does the initiative involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	No		
6	Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	No		
7	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.	No		
8	Will the initiative require you to contact individuals in ways which they may find intrusive i.e. invasive, indiscreet, interfering or upsetting?	No		

If all questions have been answered 'no' a copy of this document should be retained in accordance with our records retention policies and as the initiative develops reference made to the screening questions in case any answers change to 'yes'. If any question has been answered 'yes' please continue to complete the rest of this template.

Step one – Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

You need to check whether your processing is on the list of types of processing which automatically require a DPIA. If not, you need to screen for other factors which might indicate that it is a type of processing which is likely to result in high risk.

What is the aim of the project? – Microsoft Teams is part of Office 365 and allows schools to communicate with staff, School Governors, parents and other key stakeholders.
Using Microsoft Teams it is also possible to set up a 'Live Event' whereby members of staff can present live to viewers who can be invited by an invite link. The event is one-way only and may be suitable for schools to deliver messages to large numbers, e.g. a virtual school assembly.
The Microsoft Teams app enables schools to:

(1) Engage with others from anywhere. (2) Meet from anywhere with any number. (3) Call from anywhere. (4) Collaborate from anywhere.

The use of Microsoft Teams will help the school to deliver a cost effective solution to meet the needs of the business.

The school will be complying with Safeguarding Vulnerable Groups Act and Working together to Safeguard Children Guidelines (DfE) and will undertake the following processes:

1. Collecting personal data
2. Recording and organising 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 low 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

Microsoft Teams 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 two - Describing 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?**
- **What types of processing identified as likely high risk are involved?**

The Privacy Notice (Pupil) for the school provide the legitimate basis of why Newbold and Tredington C of E Primary School collects data. The lawful basis in order to process personal data inline with lawfulness, fairness and transparency principle is as follows:

6.1 (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
6.1(c) processing is necessary for compliance with a legal obligation to which the controller is subject
6.1 (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
The school has highlighted consent as the lawful basis by which it process this personal data as parents have given permission for school to use the information.

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 the the school's Data Retention Policy.

What is the sources of the data?
Pupil information is collected via data collection forms when a child joins the school , pupil update forms the school, issue at the start of the year and Common Transfer File (CTF) or secure transfer from previous schools. Pupil information also includes classroom work, assessment and reports.

Parental/guardian information is obtained by the parent/guardian providing personal data relating to pupil name, their relationship to the child, first and last name of the parent/guardian and email address. This is provided by an apps consent form issued to the parent /guardian.

Will you be sharing data with anyone?
Newbold and Tredington C of E Primary School routinely shares pupil information with the relevant staff within the school, schools that the pupil attends after leaving, schools within the consortium for moderation purposes, the Local Authority, the Department for Education, Health Services, Learning Support Services, Management Information Systems and various third parties including Seesaw.

What types of processing identified as likely high risk are involved?
Transferring of personal data from school to the cloud. Storage of personal data in the cloud.

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.

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 is collected and used and how often?**
- **How often?**
- **How long will you keep the data for?**

What is the nature of the data?

Individuals are pupils at the school and would be considered as vulnerable subjects. Other data subjects would include staff who are employed by the school. The school is the data controller and therefore has control over the data belonging to the data subjects.

Individuals have some control over this data processing under the individual data protection rights. i.e., Where data is processed for the purposes of fulfilling a public task, staff and pupils (or parents/carers on their behalf) can object to the processing of their information in this way. The school will weigh up the interests of the individuals in accordance with their interests, rights and freedoms and balance this against the school's legitimate purposes for processing the data.

Staff are constantly observing and assessing the children in their care. Newbold and Tredington C of E Primary School takes photographs and videos as evidence of the children's achievements and experiences. The school then use these to assess and monitor each child's progress and identify areas for development.

A Learning Journal is a record of each child's learning and shows a snap shots of children's achievement and progress in relation to the Early Years Foundation Stage (EYFS). Not every activity a child does will be recorded, staff will focus on significant moments in each child's learning.

Seesaw will be monitored by the headteacher.

Special Category data

Some personal data collected falls under the GDPR special category data. When capturing images of the child this will identify the race; ethnic origin and health.

How much data is collected and used and how often?

Personal data is collected for each pupil enrolled at Newbold and Tredington C of E Primary School.

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 consider the data retention period as outlined in the IRMS Information Management Toolkit for Schools and within the schools Data Retention Policy.

Currently, the school has limited online learning resources. Using this data processor will enable the school to fulfil their duty in providing high quality education remotely and assist learners with their learning.

Microsoft Teams 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 the relationship with individuals?**
- **How much control will they have?**
- **Would they expect you to use their data in this way?**

- **Are there prior concerns over this type of processing?**

What is the nature of the relationship with individuals?

Individuals are pupils at the school and would be considered as vulnerable subjects. Other data subjects would include staff who are employed by the school. The school is the data controller and therefore has control over the data belonging to the data subjects.

How much control will they have?

Individuals have some control over this data processing under the individual data protection rights. I.e., Where data is processed for the purposes of fulfilling a public task, staff and pupils (or parents/carers on their behalf) can object to the processing of their information in this way. The school will weigh up the interests of the individuals in accordance with their interests, rights and freedoms and balance this against the school's legitimate purposes for processing the data.

Would they expect you to use their data in this way?

Individuals are likely to expect the use of their data in this way, as the expectation is that education will continue during periods of self-isolation or in the event of a local/national lockdown / individuals will expect their data to be used in this way for the purposes of providing their child with learning resources to assist with their education. Individuals will be informed via the privacy notice.

Processing using a learning platform is not a novel processing activity and the majority of online learning platforms are well-established.

Currently, the school has limited online learning resources. Using this data processor will enable the school to fulfil their duty in providing high quality education remotely/assisting learners with their learning.

Are there prior concerns over this type of processing?

Newbold and Tredington C of E 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: Microsoft Teams sits within Office Microsoft 365. Office Microsoft 365 sits within Microsoft Azure which provides a secure cloud based service

ISSUE: Transfer of data between the school and the cloud
RISK: Risk of compromise and unlawful access when personal data is transferred.
MITIGATING ACTION: Encryption is identified in the GDPR as a protective measure that renders personal data unintelligible when it is affected by a breach
Microsoft products and services such as Azure, Dynamics 365, Enterprise Mobility + Security, Office Microsoft 365, SQL Server/Azure SQL Database, and Windows 10 offer robust encryption for data in transit and data at rest
Microsoft Teams encrypts data in transit and at rest and uses Secure Real-time Transport Protocol (SRTP) for video, audio, files, chat, and desktop sharing

ISSUE: Use of third party sub processors?
RISK: Non compliance with the requirements under GDPR
MITIGATING ACTION: Microsoft shares data with third parties acting as its sub processors to support functions such as customer and technical support, service maintenance, and other operations
Any subcontractors to which Microsoft transfers Customer Data, Support Data, or Personal Data will have entered into written agreements with Microsoft that are no less protective than the Data Protection Terms of the Online Services Terms

ISSUE: Understanding the cloud based solution chosen where data processing/storage premises are shared?
RISK: The potential of information leakage.

MITIGATING ACTION: Microsoft products and services such as Azure, Dynamics 365, Enterprise Mobility + Security, Office Microsoft 365, SQL Server/Azure SQL Database, and Windows 10 offer robust encryption for data in transit and data at rest

I**SSUE:** 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: Microsoft currently only promise to store Microsoft Teams data within the EU. Please note that they don't tell you which country or offer an option to pick a specific country (e.g. UK) However, they do have a level of granularity for some parts of Office 365 (Exchange Online, SharePoint, etc) as follows:
(1) Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments);
(2) SharePoint Online site content and the files stored within that site;
(3) files uploaded to OneDrive for Business, and;
(4) project content uploaded to Project Online
Nevertheless, in any event, Microsoft will ensure that transfers of personal data to a third country or an international organisation are subject to appropriate safeguards as described in Article 46 of the GDPR

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. 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: 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. If this includes children's data the school will apply appropriate security measures

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, Microsoft makes available to schools, as data controllers, the personal data of its data subjects and the ability to fulfil 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 Microsoft's role as a processor

If Microsoft receive a request from the school's data subjects to exercise one or more of their rights under the GDPR, Microsoft redirect the data subject to make its request directly to the data controller, i.e. the school. The Office 365 Data Subject Requests Guide provides a description to the data controller on how to support data subject rights using the capabilities in Office 365

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: Implementing data retention effectively in the cloud
RISK: GDPR non-compliance
MITIGATING ACTION: As set out in the Data Protection Terms in the Online Services Terms, Microsoft will retain Customer Data for the duration of the school's right to use the service and until all the school's data is deleted or returned in accordance with the school's instructions or the terms of the Online Services Terms

At all times the school will have the ability to access, extract, and delete personal data stored in the service, subject in some cases to specific product functionality intended to mitigate the risk of inadvertent deletion

ISSUE: Responding to a data breach
RISK: GDPR non-compliance
MITIGATING ACTION: Microsoft products and services—such as Azure, Dynamics 365, Enterprise Mobility + Security, Microsoft Office 365, and Windows 10—have solutions available today to help a school detect and assess security threats and breaches and meet the GDPR's breach notification obligations

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: Microsoft provides the ability to access, export, and delete system-generated logs that may be necessary to complete a Data Subject Access Request. Examples of such data may include: (1) product and service usage data such as user activity logs; (2) user search requests and query data; and (3) data generated by product and services resulting from system functionality and interaction by users or other systems

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

ISSUE: Security of Privacy
RISK: GDPR non-compliance
MITIGATING ACTION: Microsoft is committed to helping protect the security of the school's information. In compliance with the provisions of Article 32 of the GDPR, Microsoft has implemented and will maintain and follow appropriate technical and organizational measures intended to protect Customer Data and Support Data against accidental, unauthorized, or unlawful access, disclosure, alteration, loss, or destruction.

Microsoft 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 Microsoft's data centres, infrastructure, and operations.

The following are examples of Microsoft's accreditation:

ISO 27001: is one of the most widely recognized, internationally accepted independent security standards. Microsoft 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. Microsoft 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. Microsoft has been certified compliant with ISO 27018 for its shared Common Infrastructure

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. Microsoft has SOC 1, SOC 2 and SOC 3 reports for its shared Common Infrastructure

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

Describe the purpose 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?**

What do you want to achieve?

Schools have an obligation to ensure the continuity of education in the event children are unable to attend school due to the pandemic. Engaging a third-party data processor will be necessary for us to meet this obligation.

What is the intended effect on individuals?

Children can continue with their learning from home, this will limit any disruption to their education in the event of self-isolation or closure of the school.

The overall purpose is to ensure children can still access an education in the event of a local or national lockdown and/or during periods of self-isolation.

What are the benefits of the processing – for you, and more broadly?

The benefits of processing are that pupils can work remotely, individually, using technology and results are recorded easily, allowing the teachers to process assessment/attainment data efficiently.
Targets can be set using online platforms and overall, this is in a timely manner in which to record the progress of pupils.

Step three – 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?**

Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so.

Seeking the views of individuals may not be appropriate in this scenario as this is a standard process of the school / is part of the school's contingency plan to ensure high quality education during periods of self-isolation or a national/local lockdown/ The views of the individual will be considered when seeking consent.

Who else do you need to involve within your organisation?

We will seek advice from our Data Protection Officer via this Data Protection Impact Assessment / We will consult our IT support to ensure we access a secure platform and that data is shared using secure methods.

Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Warwickshire DPO team have also been involved in the creation of this DPIA.

Step four – Access 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?**
- **If appropriate, how will you prevent the use of the technology or system beyond the purpose for which it was originally intended?**

- **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?**

What is your lawful basis for processing?

The lawful basis for processing personal data is contained in the school's Privacy Notice (Pupils). The Legitimate basis includes the following:

- Childcare Act 2006 (Section 40(2)(a))
- The Education reform Act 1988
- Education Act 1994; 1998; 2002; 2005; 2011
- Health and Safety at Work Act
- Safeguarding Vulnerable Adults Act
- Working Together to Safeguard Children Guidelines 2018 (DfE)

Our lawful basis will be public task which is essential to the running of the school.

The school has a Subject Access Request procedure in place to ensure compliance with Data Protection Law. The school will continue to be compliant with its Data Protection Policy.

Does the processing actually achieve your purpose?

The processing helps to achieve the purpose of educating pupils. The school is required to provide high quality education during periods of self-isolation or in the event of local/national lockdown. Alternative measures, such as paper assessments/quizzes can be used, but the online platform offers a simple, quick and effective tool for learning.

Is there another way to achieve the same outcome?

Alternative measures, such as paper assessments/quizzes can be used, but the online platform offers a simple, quick and effective tool for learning.

If appropriate, how will you prevent the use of the technology or system beyond the purpose for which it was originally intended?

How will you ensure data quality and data minimisation?

Only the personal data necessary for the performance of the online platform, as set out in the GDPR compliant contract, will be collected for processing. Parents/pupils will be notified via the privacy notice on the school's website

What information will you give individuals?

The right to be informed will be supported with the aforementioned privacy notices and data subjects can visit the processor's privacy notice for further information.

How will you help to support their rights?

The right to erasure will be supported where *EITHER* consent is withdraw *OR* a valid objection to the processing is received. The right to object is outlined in step 2.

The right of access will be supported by the school's subject access request procedure, published on the website. The processor contract outlines that they will help the controller to achieve compliance with data protection obligations, which will include supporting the right to access.

What measures do you take to ensure processors comply?

The right to rectification is supported in the school's annual data collection/data checking sheets. However, specifically, pupils and/or parents can update details at any point via the school's contact details. The processor allows for changes to login/account details when required.

The school will consider any other data that may need to be rectified and communicate this with the processor where this is deemed necessary.

Right to privacy may be impacted due to video communications resulting in teachers and other individuals hearing and seeing what goes on in people's homes. To mitigate this risk, individuals will have the option to/ teachers will ensure cameras and microphones are switched off.

How do you safeguard any international transfers?

Step five - Identity 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** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, medium or high
Data transfer, data compromised	Remote	Minimal	Low
Loss of password and/or loss of access to the site	Possible	Significant	Low
Data used outside the scope of its original purpose (including children using the online platform as a form of social media	Remote	Minimal	Low
Impacts on indivivual's rights to privacy	Possible	Severe	Medium

Step six - Identity 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** Eliminate, reduced or accepted	**Residual risk** Low, medium, high	**Measure approved** Yes/No

Hacking into processor site	Outline security measures from contract	Reduced	Low	Yes
Loss of login passwords/ username and/or loss of access into the site	Outline the details on how lost login details will be managed/ supported. Parents, guardians and children advised not to share passwords.	Reduced	Low	Yes
Data used outside the scope of its original purposes	The contract/agreement meets the requirements of GDPR – assurances are given in the legally binding contract for the purposes for which the data will be used/processed. School staff are briefed and made aware of the school's data protection and information security policy. For children using the function as a form of social media, rules on using the system will be in place and this will be monitored / chat functions will be disabled at all times/at the end of each lesson.	Reduced	Low	Yes
Impact on rights to privacy	Individuals will have the option to turn off their camera and mute their microphone / teachers will ensure all participants mute their microphone and turn off the camera function. Pupils will be invited to unmute their microphone when appropriate for engaging in the lessons and then asked to unmute again. Parents will be made aware of the lessons and timetables and given the opportunity to voice their concerns and exercise their right to object.	Reduced	Low	Yes

Step seven - Sign off and record outcomes		
Item	Name/date	Notes
Measure approved by:	Head teacher/DPO	Integrate actions back into project plan, with date and responsibility for completion.

Residual risks approved by:	Head teacher/DPO	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Yes	DPO should advise on compliance, step six measure and whether processing can proceed.
Summary of DPO Advice: 1. Does Seesaw provide technical capabilities to ensure the school can comply with the right of access and subject access requests? 2. Are the parents fully aware of the online platform and how to ensure that their account remains safe?		
DPO advice accepted or overused by:	Accepted	If overruled, you must explain your reasons
Comments:		
The DPIA will be kept under review by:	Head teacher/DPO	The DPO should also review ongoing compliance with DPIA