Insert School Logo Here

DPIA Screening and Advice Note – Video conferencing- use of MS Teams

Version 2.0

GUIDANCE NOTE

UK Schools are rapidly putting virtual meeting and learning platforms in place in case of a partial or full school closure as part of measures to isolate infected individuals as part of the response to the Covid-19 Pandemic. Many technology providers are providing resources and facilities to support remote working and learning, many of which are being offered to schools for free at this time.

Schools have a variety of options available to them to enable the staff to communicate with other school staff, pupils or the wider school community. Each school must make the decision to ensure the needs of their particular group of staff, pupils and parents are communicated with in the most appropriate way possible. It is important to note that no provider is the 'wrong' provider in these circumstances and likewise, no particular provider is 'approved' or 'recommended' as each school is unique in its requirements/resources.

This document has been prepared by the GDPR for Schools Teams, IT Support and Safeguarding Teams in Derbyshire County Council on behalf of all Derbyshire Schools as a guide only. Schools are responsible for ensuring that Safeguarding and Data Protection measures are in place to mitigate risk, put appropriate procedures, safeguards and codes of conducts in place and communicate these to all users of video conferencing as appropriate. We are aware that schools may find it too onerous to carry out a full Data Protection Impact Assessment at this time so have also produced a simple DPIA screening document that schools may use. Detail regarding Data Protection risk analysis is appended to the end of this document.

Safeguarding

Safeguarding of individuals, particularly pupils, remains the utmost priority for schools. Firstly, the school should distinguish between the considerations for the use of video-conferencing service for use by staff at a school only *and use by staff to contact pupils or their families*. Considerations of the risks and benefits of these two different uses will be considerably different.

Video conferencing platforms can be an invaluable tool. However, schools should be aware that a heightened sense of urgency can also lead to an increased risk regarding safeguarding and data protection.

Some video conferencing tools are well established, and may already be in current use (e.g. Microsoft Teams) – others may have seen their popularity and uptake increase (e.g. Zoom). Whilst schools remain free to choose a particular provider, schools should first consider using the Teams app, as part of their Microsoft Office package; it is an effective means of communicating and has robust privacy settings.

Safeguarding and child protection remains as important in this environment as anywhere else, and staff members should apply their school's safeguarding guidance to online learning, just as they would to classroom working - staff who become aware of any child protection concerns should continue to follow their setting's established safeguarding procedures.

It should be noted that a school maintains, in the current circumstances, a public interest to educate and safeguard the pupils under its care and every effort must be made to continue supporting children and families, through whichever resources it finds most effective.

When working remotely, schools should consider the following safeguarding issues;

- Under no circumstances is it appropriate for staff members to hold one-to-one videoconferences with a pupil due to safeguarding risk.
- Staff should separate their remote learning account from their personal online profiles and use a duplicate of the staff notice image for the platform profile picture. Set up school accounts for any online platforms you used and check the privacy settings.
- Make sure any phone calls are made from a blocked number so the staff members personal contact details are not visible. Where necessary, schools should consider the purchase of dedicated mobile telephones for the purpose of teacher to pupil/family communications and as an emergency contact for the school number e.g. for DSL use.
- Never share any personal information e.g. personal telephone number, email accounts, Facebook and other social media links. Staff should never use personal social media accounts as a 'short cut' to communicate with parents and pupils.
- For the purposes of video-conferencing, particularly with primary school age pupils, it may be more appropriate to use the parents' or guardians' account, rather than a child's, to deliver lessons. Use parents' or carers' email addresses or phone numbers to communicate with children, unless this poses a safeguarding risk**.**
- Ensure staff members work against a neutral background. Staff should present themselves as they would if they were giving a face-to-face lesson, in dress and in manner.
- Where lessons are delivered to a class, parents/carers and pupils should be provided with safeguarding and etiquette guidance in advance of the lesson For example, the pupil must take lessons in a room with an open door and parents/guardians must provide that one of them or for a trusted adult shall be in the same room as the pupil while the lesson takes place.

All staff should be aware of their settings safeguarding and child protection policy and procedures, even when working remotely. Ensure that staff members are able to contact the Designated Safeguarding Lead (DSL) or, in the event of the DSL being unavailable, deputy DSL, should they have any concerns about a child. Examples of potential concerns may include;

- a staff member seeing, or hearing, a concern during an online lesson
- a disclosure, made by a pupil, during a phone call, via email or in the course of a lesson.

When making contact directly with children, as a means of checking on their welfare, schools should consider which methods are most appropriate and applicable.

Schools should not record online lessons – these are defined as protected data under current legislation and cannot be collected, stored or retrieved without parental permission or in any other way that does not comply fully with the requirements of the Date Protection Act (2018).
Staff members are, however, advised to record the length, time, date and attendance of any sessions held.

Further information can be found at:

https://learning.nspcc.org.uk/news/2020/march/undertaking-remote-teaching-safely/
https://swgfl.org.uk/resources/safe-remote-learning/

Data Protection

The requirements of the GDPR to assess the lawful basis for Data Sharing and the Data Protection suitability of providers of services still apply in the event of school closures. This document examines the suitability of Microsoft Teams to provide video conferencing and sets out steps for schools to take. Due to the urgent need to issue guidance for schools, and the exceptional circumstances, schools may not go through the same consultation and approval process as would normally be undertaken for a project of this nature. Schools should ensure that they address the issues in the Action List as part of their Data Protection work.

Microsoft Teams

Most schools already have access to Microsoft Teams via their Office 365 Licence. This enables staff to set up Teams to video-conference with each other. It is also possible to invite pupils/parents who can join Teams via a 'guest invite'. Invites to attendees should be sent out by email using "BCC" to prevent email addresses for private individuals inadvertently being shared with all attendees (Helpful hint- if you don't have the function to set up a Teams Meeting using the Outlook programme, create the meeting in Teams and invite one colleague, then go to your Outlook sent items folder- you will see an email containing a hyperlink has been sent to the colleague- cut and paste this link into an email where you can use the BCC function)

It is also possible to set up a 'Live Event' whereby member/s of staff can present live to viewers who can be invited by an invite link. The event is one-way only so there is no ability to see the viewers of the event- this is suitable for schools to deliver messages to large numbers, e.g. a virtual school assembly. There is a small charge for this and DCC IT Services can assist any schools that wish to use this service. The recommendation is that Teams should be used unless the school does not subscribe to a Microsoft 365 tenancy agreement. Teams by default is disabled for student accounts in Office365, however staff members can still invite external guests through providing a guest link by secure email to external participants whether they use Microsoft365 or not.

DPIA Screening of MS Teams

Name of School	
Document Prepared by	**Data Protection Officer and Mrs Teresa Bosley**
Reviewed by DPO	**Yes – produced by DCC**
Date of Screening	**February 2021**
Review Date	**February 2022**

The school plans to use Microsoft Teams to deliver video-conferencing facilities for the following purposes:

- Online teaching of groups of pupils
- Staff and Governor meetings

The following safeguards have been put in place:

- Child Protection Policy Addendum document has been adopted by the school
- Parents, staff and pupils have been given guidance on safe use of the platform

Screening questions

Will the project involve the collection of new information about individuals? If yes, please detail the information to be collected.
Yes, data will be shared with the provider to allow users to have accounts. This data will be limited to the minimum necessary for accounts to be set up (usually first and last name and email address).

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? If yes, please detail which organisations will be provided with access.
Yes. The school will be sharing data with the provider who will be data processor.

Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition. If yes, please detail the new technology, below.
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.

Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them? If yes, please describe the impact, below.
No.

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 private. If yes, please describe the information to be collected, below.
The information indirectly relates to children who are identified under the GDPR as requiring extra safeguards to protect their data. However, the only information that is shared with the provider is the name and email address of the person that is set up on the account. The content of the video conference is processed by the provider and this may include children's data.

What is the lawful basis of the processing?
The lawful basis for processing this information is that it is necessary for a task in the public interest. Special category data should not be processed but if any special category data is processed, then it is justified as necessary for substantial public interest. The processing is also justified under Schedule 1 Section 18 of the Data Protection Act 2018- "safeguarding of children and individuals at risk". In the circumstances, the controller cannot be reasonably expected to obtain the consent of the data subject before processing.

Note regarding Consultation

Due to the time constraints and the need to quickly put systems in place, there will be no consultation at this time. Parents and pupils will be informed by email that the new provider will be used. The provider will be added to the relevant Privacy Notices as soon as possible. When normal teaching resumes, the school will no longer need to use this service. For Primary School pupils, invites to meetings will appear on the class page. A reminder email will be sent to parents' email addresses, pupils will not be contacted directly.

Risk/Benefit of this Project

It is important to note that the use of Teams in itself does not necessarily engage in 'high risk' processing. It is the use of the platform to work with pupils remotely that may result in safeguarding and data protection risks. Due Diligence has been carried out on the Microsoft platform to assess risk (the detail of which is in the Appendix of this document) but the greatest reduction of risk will be to ensure that users of Teams are given clear guidance on safe use of the platform. This includes guidance as set out in the note at the beginning of this document, but also guidance on the safe use of IT, including ensuring passwords are secure to protect against unauthorised access to systems.

Key risk mitigations are:

- The provider/s will be given the minimum amount of data needed in order to use the system.
- Checking the Administrative Centre for the Microsoft account- ensure account settings are up to date and the location of data storage.
- Users will be asked to keep their passwords safe as per the IT Acceptable Use Policy.
- Meetings will be secured by private passwords so only invitees can attend the meeting.
- Privacy settings as recommended by the provider will be used to minimise any risk to privacy.
- Safeguarding protocols will be put in place and communicated to all users as appropriate.
- For Primary School pupils, invites to meetings will appear on the class page. A reminder email will be sent to parents' email addresses, pupils will not be contacted directly.

Actions to take

1. Obtain prior approval of DPO and Data Protection Governor if possible.
2. Check the Administrative Centre for the Microsoft account- check where the data is stored, and which staff have which level of access privileges and that these are up to date (you may need your IT Technician to help with this).
3. Ensure name and email address details for users are up-to-date if possible- e.g. phone users to check correct address. Ensure parents/carers are informed and engaged as much as possible and that contact with pupils is done via parent/carer supervision wherever possible.
4. Add processor to pupil and workforce privacy notice.
5. Add processor to data map.
6. Retain data in line with guidance in Retention schedule and delete or download data to school systems at the end of period of use. School to request provider/s delete data at the end of the use of the platform/s
7. Keep this document under review and check use of provider/s is in accordance with the intentions set out in this document.

Data Protection Detail Appendix

A. Evidence of due diligence of supplier

The text and links at https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dpia-office365?view=o365-worldwide have been reviewed by the DPO. This contains detail regarding whether a DPIA is needed for the use of Microsoft products and sets out some of the key risks and mitigations.

Microsoft meets the following compliance measures:
FedRamp, HIPAA/HITECH, ISO 27001, ISO 27002, ISO 27018, NIST 800-171, UK G-Cloud.

Microsoft Privacy Statement

Personal data we collect

Microsoft collects data from you, through our interactions with you and through our products. You provide some of this data directly, and we get some of it by collecting data about your interactions, use, and experiences with our products. The data we collect depends on the context of your interactions with Microsoft and the choices you make, including your privacy settings and the products and features you use. We also obtain data about you from third parties.
If you represent an organization, such as a business or school, that utilizes Enterprise and Developer Products from Microsoft, please see the Enterprise and developer products section of this privacy statement to learn how we process your data. If you are an end user of a Microsoft product or a Microsoft account provided by your organization, please see the Products provided by your organization and the Microsoft account sections for more information.

You have choices when it comes to the technology you use and the data you share. When we ask you to provide personal data, you can decline. Many of our products require some personal data to provide you with a service. If you choose not to provide data required to provide you with a product or feature, you cannot use that product or feature. Likewise, where we need to collect personal data by law or to enter into or carry out a contract with you, and you do not provide the data, we will not be able to enter into the contract; or if this relates to an existing product you're using, we may have to suspend or cancel it. We will notify you if this is the case at the time. Where providing the data is optional, and you choose not to share personal data, features like personalization that use such data will not work for you.

How we use personal data

Microsoft uses the data we collect to provide you with rich, interactive experiences. In particular, we use data to:

- Provide our products, which includes updating, securing, and troubleshooting, as well as providing support. It also includes sharing data, when it is required to provide the service or carry out the transactions you request.
- Improve and develop our products.
- Personalize our products and make recommendations.
- Advertise and market to you, which includes sending promotional communications, targeting advertising, and presenting you with relevant offers.
- We also use the data to operate our business, which includes analyzing our performance, meeting our legal obligations, developing our workforce, and doing research.

In carrying out these purposes, we combine data we collect from different contexts (for example, from your use of two Microsoft products) or obtain from third parties to give you a more seamless, consistent, and personalized experience, to make informed business decisions, and for other legitimate purposes.

Our processing of personal data for these purposes includes both automated and manual (human) methods of processing. Our automated methods often are related to and supported by our manual methods. For example, our automated methods include artificial intelligence (AI), which we think of as a set of technologies that enable computers to perceive, learn, reason, and assist in decision-making to solve problems in ways that are similar to what people do. To build, train, and improve the accuracy of our automated methods of processing (including AI), we manually review some of the predictions and inferences produced by the automated methods against the underlying data from which the predictions and inferences were made. For example, we manually review short snippets of a small sampling of voice data we have taken steps to de-identify to improve our speech services, such as recognition and translation.

Reasons we share personal data

We share your personal data with your consent or to complete any transaction or provide any product you have requested or authorized. We also share data with Microsoft-controlled affiliates and subsidiaries; with vendors working on our behalf; when required by law or to respond to legal process; to protect our customers; to protect lives; to maintain the security of our products; and to protect the rights and property of Microsoft and its customers.

How to access and control your personal data

You can also make choices about the collection and use of your data by Microsoft. You can control your personal data that Microsoft has obtained, and exercise your data protection rights, by contacting Microsoft or using various tools we provide. In some cases, your ability to access or control your personal data will be limited, as required or permitted by applicable law. How you can access or control your personal data will also depend on which products you use. For example, you can:

- Control the use of your data for interest-based advertising from Microsoft by visiting our opt-out page.
- Choose whether you wish to receive promotional emails, SMS messages, telephone calls, and postal mail from Microsoft.
- Access and clear some of your data through the Microsoft privacy dashboard.

Not all personal data processed by Microsoft can be accessed or controlled via the tools above. If you want to access or control personal data processed by Microsoft that is not available via the tools above or directly through the Microsoft products you use, you can always contact Microsoft at the address in the How to contact us section or by using our web form.

We provide aggregate metrics about user requests to exercise their data protection rights via the Microsoft Privacy Report.

Cookies and similar technologies

Cookies are small text files placed on your device to store data that can be recalled by a web server in the domain that placed the cookie. We use cookies and similar technologies for storing and honoring your preferences and settings, enabling you to sign in, providing interest-based advertising, combating fraud, analyzing how our products perform, and fulfilling other legitimate purposes. Microsoft apps use additional identifiers, such as the advertising ID in Windows described in the Advertising ID section of this privacy statement, for similar purposes.

We also use “web beacons” to help deliver cookies and gather usage and performance data. Our websites may include web beacons, cookies, or similar technologies from third-party service providers.

You have a variety of tools to control the data collected by cookies, web beacons, and similar technologies. For example, you can use controls in your internet browser to limit how the websites you visit are able to use cookies and to withdraw your consent by clearing or blocking cookies.

Products provided by your organization—notice to end users

If you use a Microsoft product with an account provided by an organization you are affiliated with, such as your work or school account that organization can:

- Control and administer your Microsoft product and product account, including controlling privacy-related settings of the product or product account.
- Access and process your data, including the interaction data, diagnostic data, and the contents of your communications and files associated with your Microsoft product and product accounts.

If you lose access to your work or school account (in event of change of employment, for example), you may lose access to products and the content associated with those products, including those you acquired on your own behalf, if you used your work or school account to sign in to such products.

Many Microsoft products are intended for use by organizations, such as schools and businesses. Please see the Enterprise and developer products section of this privacy statement. If your organization provides you with access to Microsoft products, your use of the Microsoft products is subject to your organization's policies, if any. You should direct your privacy inquiries, including any requests to exercise your data protection rights, to your organization’s administrator. When you use social features in Microsoft products, other users in your network may see some of your activity. To learn more about the social features and other functionality, please review documentation or help content

specific to the Microsoft product. Microsoft is not responsible for the privacy or security practices of our customers, which may differ from those set forth in this privacy statement.
When you use a Microsoft product provided by your organization, Microsoft's processing of your personal data in connection with that product is governed by a contract between Microsoft and your organization. Microsoft processes your personal data to provide the product to your organization and you, and for Microsoft's legitimate business operations related to providing the product as described in the Enterprise and developer products section. As mentioned above, if you have questions about Microsoft's processing of your personal data in connection with providing products to your organization, please contact your organization. If you have questions about Microsoft's legitimate business operations in connection with providing products to your organization, please contact Microsoft as described in the How to contact us section. For more information on our legitimate business operations, please see the Enterprise and developer products section.

For Microsoft products provided by your K-12 school, including Microsoft 365 Education, Microsoft will:

- not collect or use student personal data beyond that needed for authorized educational or school purposes;
- not sell or rent student personal data;
- not use or share student personal data for advertising or similar commercial purposes, such as behavioral targeting of advertisements to students;
- not build a personal profile of a student, other than for supporting authorized educational or school purposes or as authorized by the parent, guardian, or student of appropriate age; and
- require that our vendors with whom student personal data is shared to deliver the educational service, if any, are obligated to implement these same commitments for student personal data.

Microsoft meets with the GDPR's Privacy by Design Requirement with the Microsoft Security Development Lifecycle (SDL)

Privacy requirements are defined and integrated in the SDL, the software development process that helps developers build more secure products and services. The SDL helps address data protection and privacy requirements including effective privacy reviews of each release of a Microsoft product or service.

B: Supplier Contract investigations

The GDPR requires controllers (such as organizations using Microsoft's enterprise online services) only use processors (such as Microsoft) that provide sufficient guarantees to meet key requirements of the GDPR. Microsoft has taken the proactive step of providing these commitments to all Volume Licensing customers as part of their agreements.

"How does Microsoft help me comply?
Microsoft provides tools and documentation to support your GDPR accountability. This includes support for Data Subject Rights, performing your own Data Protection Impact Assessments, and working together to resolve personal data breaches.

What commitments are in the GDPR Terms?
Microsoft's GDPR Terms reflect the commitments required of processors in Article 28. Article 28 requires that processors commit to:

- *Only use subprocessors with the consent of the controller and remain liable for subprocessors.*
- *Process personal data only on instructions from the controller, including with regard to transfers.*
- *Ensure that persons who process personal data are committed to confidentiality.*
- *Implement appropriate technical and organizational measures to ensure a level of personal data security appropriate to the risk.*
- *Assist controllers in their obligations to respond to data subjects' requests to exercise their GDPR rights.*
- *Meet the breach notification and assistance requirements.*
- *Assist controllers with data protection impact assessments and consultation with supervisory authorities.*
- *Delete or return personal data at the end of provision of services.*

Support the controller with evidence of compliance with the GDPR.

Under what basis does Microsoft facilitate the transfer of personal data outside of the EU?

Microsoft Blog Statement July 2020:

"Today the Court of Justice of the European Union has issued a judgment relating to a case examining data transfers from the EU. We want to clarify the impact of this decision for our customers.

We confirm that all our customers can continue to use Microsoft services, in full compliance with European law. The court ruling does not change the ability to transfer data between the EU and the United States using the Microsoft cloud.

For years, Microsoft has provided customers with high levels of protection for both the Standard Contractual Clauses (SCC) and the Privacy Shield for all data transfers. Although today's ruling invalidated the use of the Privacy Shield, the SCCs remain valid. Our customers are already protected by SCCs for using the Microsoft cloud and related data transfers.

Furthermore, today's ruling does not change the data flows of our services to Consumers. We transfer data between users, for example, when a person sends email or other online content to another person. We will continue to do so in accordance with today's decision and with future and further guidelines from the EU data protection authorities and the European Data Protection Board.

In addition to supporting customers who transfer data between the EU and the United States, we will continue to work proactively with the European Commission and the United States government to address the issues raised by the ruling. The Court raised some important arguments that Governments must consider when establishing a data transfer policy between countries. We will continue to do our part by committing ourselves to work with European and American governments and regulators to address these issues. We are confident that the European Commission and the United States government will also work to address these issues and we are grateful that they are actively involved in finding solutions.

We have always worked to improve the level of protection for our customers. We were the first cloud company to work with European data protection authorities for Model Clauses approval in Europe and the first company to adopt new technical standards for the Privacy of Cloud services. We have accepted the Privacy Shield as a successor to Safe Harbor after the cancellation of this model and we have extended the GDPR key rights to our Customers all over the world.

Finally, we will continue to take measures to defend the rights of our customers. We filed a lawsuit to challenge orders that required access to people's data or to protect our ability to inform users of pending requests, bringing the case to the United States Supreme Court . Thanks to our actions, we have guaranteed greater transparency for our customers, through an agreement that has allowed us to disclose reports on the number of orders required by the United States national security. In addition to establishing new policies within the United States government that limit the use of secrecy orders.

Privacy is a continuous journey, and today's sentence is not the last word. Our customers can be confident that we will strive to ensure that their data can continue to move through our services. They can also count on the fact that we will continue our work to provide them with greater protection based on the issues raised in today's ruling and that we will collaborate with governments and those responsible for privacy policies, following the evolution of future decisions"

C: Linking the DPIA to the Data Protection Principles

Answering these questions during the DPIA process will help you to identify where there is a risk that the project will fail to comply with the GDPR or other relevant legislation, for example the Human Rights Act.

Principle 1

Lawfulness, fairness and transparency of data processing

There must be lawful basis for processing the personal data as follows;

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.

Have you identified the purpose of the project and which lawful basis applies?	E
Is the processing of the data necessary in terms of GDPR?	Yes
How will you tell individuals about the use of their personal data?	P.N. and by urgent message to users
Do you need to amend your privacy notices?	Yes
If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?	n/a
If special categories of personal data have been identified have the requirements of GDPR been met?	Yes
As the School is subject to the Human Rights Act, you also will, where privacy risk are especially high, need to consider:	
Will your actions interfere with the right to privacy under Article 8	Potentially
Have you identified the social need and aims of the project?	Yes
Are your actions a proportionate response to the social need?	Yes

Principle 2
Personal data shall be obtained only for one or more specified explicit and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Does your project plan cover all of the purposes for processing personal data?	Yes
Have you identified potential new purposes as the scope of the project expands?	Yes
Does your Privacy Notice cover all potential uses?	Yes

Principle 3
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Is the quality of the information good enough for the purposes it is used?	Yes
Which personal data could you not use, without compromising the needs of the project?	None

Principle 4
Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary?	Yes
How are you ensuring that personal data obtained from individuals or other organisations is accurate?	Interaction with school MIS. School will check email addresses wherever reasonably practicable to do so.

Principle 5
Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary.

What retention periods are suitable for the personal data you will be processing?	As per school policy
Are you procuring software that will allow you to delete information in line with your retention periods?	Yes

Principle 6

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Do any new systems provide protection against the security risks you have identified?	Yes
What training and instructions are necessary to ensure that staff know how to operate a new system securely?	None

Rights of Data Subjects and Privacy by Design

Will the systems you are putting in place allow you to respond to subject access requests?	Yes
Will the system allow compliance with individual rights under GDPR, in particular the right to be informed, the right to rectification and the right to ensure (right to be forgotten).	Yes
If the project involves marketing, have you got a procedure for individuals to opt in to their information being used for that purpose?	n/a

Transferring data outside European Economic Area

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data**.**

Will the project require you to transfer data outside of the EEA?	Possibly
If you will be making transfers, how will you ensure that the data is adequately protected?	Standard Contractual Clauses and security of processing confirmation by Microsoft following "Schrems II" Judgment.

D: Detailed Risks and Mitigations of Project

Identified risk	Detail of risk	Controls to be implemented	Proposed Mitigation
Lawfulness of processing	No new data is being generated or processed by this project. The existing lawful basis for each type of processing currently being done on Schools network shares will also apply to the same activity on Microsoft Teams. The school has identified Public Task as a lawful basis for the act of processing data on Microsoft Teams.	HT to control who is in attendance, the agenda for the meetings, and to host the meeting from an account that has been set with appropriate security settings to minimise data collection/processing, and restrict what facilities are available to attendees in the meeting. If your organization or users engage with Microsoft to receive, support related to Microsoft products and services some of this data may contain personal data. For more information, see Microsoft Support and Professional Services Data Subject Requests for the GDPR.	Lowers risk
Fairness and transparency of processing	Low risk that attendees use Microsoft Teams for a new data processing activity that has not been screened for GDPR issues, and that is not added to the Record Of Processing Activities, and not covered by privacy notices.	Disabled ability to screen share for all but HT/Host, disabled file sharing, and chat. HT only to share relevant presentations, and to keep meetings focused on agenda.	Lowers risk
Data minimisation	Low risk - Live video feeds and audio streams are being processed during a meeting, but this is not retained by Microsoft Teams once a meeting ends.	As above, meetings locked down to live video and audio. Once the meeting is over, attendees will not have any new data stored on device from meeting.	Lowers risk
Maintaining accurate and up to date data	Low risk that the HT details will change and need to be changed in the hosting account.	Microsoft Teams hold limited personal data for account holder – If HT details change, account will need to be deleted and reassigned to new HT. This is possible and Microsoft Teams will permanently delete accounts once they have been deleted by the user.	Lowers risk
Ability for data subjects to opt out or object to processing	Unable to allow data subjects the right to object to processing.	We accept that it will not be possible for data subjects to opt out of having their basic meta data processed on Microsoft Teams, but have ensured where possible, additional processing has been opted out. Privacy policy https://privacy.microsoft.com/en-gb/privacystatement Host will invite attendees to Microsoft Teams meetings via email. Email provider will have a trail of all invites sent out and can request Microsoft Teams delete and stored meta data.	Lowers risk

		Meeting Metadata: Topic, Description (optional), participant IP addresses, device/hardware information To make a request, please contact our Privacy Team The school will ensure that individuals (staff) are aware of their rights under data protection legislation, including the right to object where the lawful basis is a public task duty.	
Ability to respond to subject access requests	Moderate risk that ICT admin staff will not be able to locate all relevant personal information stored on Microsoft Teams to be able to respond to an SAR.	We have to request any information from Microsoft Teams as we have no access to this. You can request a copy of the personal data. https://blogs.microsoft.com/datalaw/our-practices/	Lowers risk
Rights of the data subjects	Low risk of difficulty complying with Right to Rectification and Right to Erasure as only basic information is stored.	From Privacy policy - https://Microsoft Teams.us/privacy Erasure**:** You can request that we erase some or all of your personal data from our systems. Microsoft Teams DPA also includes: Following completion of the Services, at Customer's choice, Microsoft Teams shall return or delete the Personal Data, except as required to be retained by law, rule or regulation that is binding upon Microsoft. If Customer and Microsoft Teams have entered into Standard Contractual Clauses (Transfers of Personal Data), the parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Microsoft Teams to Customer only upon Customer's request.	Lowers risk
Transfers to third parties	Low risk that staff might accidentally share personal data with another individual or organisation.	Attendees have to be invited in. All attendees and host can see all participants and should screen to ensure everyone present is meant to be there. Microsoft Teams has settings to allow the invitee into the conference from the virtual waiting room and to prevent screen share and other functionalities. These can be disabled by host. This gives the host greater ability to ensure those attendees are legitimately invited to the meeting and prevent unauthorised access. The host can lock the session after attendees have entered to prevent further access. Microsoft Teams have stated: in a meeting where all of the participants are using Microsoft Teams clients, and the meeting is not being recorded, we encrypt all video, audio,	Lowers risk

		screen sharing, and chat content at the sending client, and do not decrypt it at any point before it reaches the receiving clients.	
Transfers outside the EEA or to international organisations	Medium risk that we will have an issue with storing data inside the EEA, rather than inside the UK, after Brexit transition ends.	The account data held on the host/HT account may be held outside of the EU, as is meta data from meeting attendees. Microsoft Teams use the Standard Contractual Clauses to provide a mechanism to comply with GDPR requirements.	Lowers risk.
Retention and deletion	Medium risk that the school will struggle to identify and delete all personal information held on Microsoft Teams at the end of its retention period. Guests who have joined meetings hosted by HT	Host to keep a log of all attendees at every meeting, date and time of meeting, to ensure we can track all participants and request meta data is deleted.	Lowers risk
Data security	Low risk that an attendee might share personal data with the wrong person in error.	Host to screen all attendees before meeting commences.	Lowers risk
Data breach	Medium risk that an attendee video conferencing from home might accidentally disclose their own, or other household members' personal information to colleagues. This could happen inadvertently, such as by having personal information within camera range.	Attendees to be advised on best practice for attending VC from home – Behind closed door away from other household members, minimal personal affects in background etc. Ensure staff have received guidance around homeworking. (Refer to safeguarding advice above)	Lowers risk.
Unauthorised use	Medium risk of issues if staff use Microsoft Teams video conferencing facilities for non-work purposes whilst at home.	Although we have set up an account with restrictions for our Host/HT, there is nothing to stop others setting up their own personal accounts. Advise against this. School have an AUP that discusses the use of school personal data for private use.	Lowers risk.
Security of processing	Low risk that a data breach occurs because ICT admin staff are not sufficiently trained and familiar with Microsoft Teams to be able to correctly configure all features for optimum privacy.	Hosts will be given time to investigate all settings available to the host account and make sure it is restricted as much as possible. Training regarding how to use Microsoft Teams will be undertaken by staff who will have access to the service.	Lowers risk.