Video conferencing (inc. Zoom) use in Schools during Covid- 19 Closure

Version 1.0

GUIDANCE NOTE

UK Schools have had a compulsory school closure as part of the Government Strategy to respond to Covid-19. 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. Many schools are using or considering using Zoom. Zoom is a video-conferencing facility that has become incredibly popular across a variety of settings, including use in Education across the world.

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. There is a full DPIA appended to this document for schools that wish to use Zoom. However, we are aware that schools may find it too onerous to carry out a full DPIA at this time so have also produced a simple DPIA screening document that schools may use.

Safeguarding

Safeguarding of individuals, particularly pupils, remains the utmost priority for schools. Firstly, the school should distinguish between the considerations for the use of Zoom or other 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. However, for schools that have already begun using Zoom or similar audio visual tools (FaceTime, Skype), this document provides some of the necessary guidance and procedural framework.

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 video conferences 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. You should set up school accounts for any online platforms you use 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, use the parents' or guardians' own account, where possible, 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 premises as the pupil while the lesson takes place.

All staff should be aware of their settings safeguarding and child protection policy and procedures. 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 two main providers, Microsoft Teams and Zoom, 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, there is a DPIA for Zoom appended to this document (this 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.

Which provider to use?
There are several providers available. The two most common providers have been considered but the principles apply whichever provider a school chooses to use.

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'.
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 Microsoft 365 or not.

Zoom
The popularity of Zoom has 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 at https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/ and published guidance for administrators on setting up and securing a virtual classroom https://zoom.us/docs/doc/School%20Administrators%20Guide%20to%20Rolling%20Out%20Zoom.pdf. Further reassurance was provided in an email by Zoom on 9/4/20 (see Appendix).

Please be aware; several, high profile security breaches on Zoom have been the result of data being wrongfully shared by users (https://www.tes.com/news/coronavirus-head-warns-pupils-after-zoom-porn-attack) – 'The (details, date and time of the) meeting was shared freely over Twitter and wasn't password protected'. Schools should always 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.

DPIA Screening Template

Name of School	**MORTON PRIMARY SCHOOL**
Document Prepared by	**JANE RADFORD**
Reviewed by DPO	**YES**
Date of Screening	**04.05.2020**
Review Date	**04.05.2021**

The school plans to use 'ZOOM' to deliver video-conferencing facilities for the following purposes: CLASSROOM LEARNING, & KEEPING IN TOUCH WITH PUPILS. The following safeguards have been put in place:

- Under no circumstances is it appropriate for staff members to hold one-to-one video conferences 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. You should set up school accounts for any online platforms you use 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, use the parents' or guardians' own account, where possible, 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 premises as the pupil while the lesson takes place.

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 text message 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.

The DPO advises that the use of Video Conferencing (particularly for contact with pupils) should be restricted in as far as is possible. There are a number of issues that have been flagged, such as "Zoombombing" and forcing staff to use Video Conferencing when there is alternative provision available. The school have accepted the risks despite and wish to continue with the use of Video Conferencing using Zoom.

However, because the school takes data protection requirement seriously, this document outlines the reasoning behind the decision, an action plan and also sets out the terms and conditions and privacy notice of the provider.

Reason for this decision:

- The provider/s will be given the minimum amount of data needed in order to use the system.
- There is an urgent need to share this data to deliver the statutory functions of the school in exceptional circumstances.
- 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 (see Appendix).
- Safeguarding protocols will be put in place and communicated to all users as appropriate.

Actions to take

1. Obtain prior approval of DPO and Data Protection Governor if possible.
2. 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.
3. Add processors to pupil and workforce privacy notice.
4. Add processors to data map.
5. 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
6. Keep this document under review and check use of provider/s is in accordance with the intentions set out in this document.

Appendix A: Evidence of due diligence of supplier/s

The Terms and Conditions and Privacy Policies of the following have been checked:
Microsoft
https://privacy.microsoft.com/en-gb/privacystatement

Zoom
https://blog.zoom.us/wordpress/2020/03/29/zoom-privacy-policy/
https://zoom.us/terms
https://zoom.us/privacy?zcid=1231&_ga=2.107193093.66078269.1585923231-2045136038.1581578314

Whilst not binding, this blog post and email below provides reassurances about the intent of Zoom to protect privacy:
https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/

From: CS Advisor <customer-success-advisor@zoom.us>
Date: 9 April 2020 at 00:18:24 BST
To: Tony Sheppard <xxxxxxxxxxxxxxxxxxxxxx@gdpr.school>
Subject: Overview of Recent Updates to Zoom
Reply-To: customer-success-advisor@zoom.us

Hi there,
As Eric shared last week, our commitment to strengthening and improving Zoom is our number one priority. I wanted to reach out with a quick overview of our latest release, and highlight the number of new enhancements created specifically for ensuring the security and privacy of our product. For more information on these changes, please reference our Release Notes.

Security Toolbar Icon for Hosts

- The meeting host will now have a Security option in their meeting controls, which exposes all of Zoom's existing in-meeting security controls one place. This includes locking the meeting, enabling Waiting Room, and more. Users can also now enable Waiting Room in a meeting, even if the feature was not turned on before the start of the meeting. For more information, please visit this recently published Blog.

Invite Button on Meeting Client Toolbar

- The button to invite others to join your Zoom meeting is now available at the bottom of the Participants panel

Meeting ID No Longer Displayed

- The meeting ID will no longer be displayed in the title bar of the Zoom meeting window. The meeting ID can be found by clicking on **Participants**, then **Invite or** by clicking on the info icon at the top left of the client window.

Remove Attendee Attention Tracking Feature

- Zoom has removed the attendee attention tracker feature as part of our commitment to the security and privacy of our customers. For more background on this change and how we are pivoting during these unprecedented times, please see a note from our CEO, Eric S. Yuan

Removal of the Facebook SDK in our iOS client

- We have reconfigured the feature so that users will still be able to log in with Facebook via their browser

File Transfers

- The option to do third-party file transfers in Meeting and Chat was temporarily disabled. Local file transfer is available with our latest release. Third-party file transfers and clickable URLs in meeting chat will be added back in an upcoming release

New Join Flow for the Web client

- By default, users will now need to sign in to their Zoom account or create a Zoom account when joining a meeting with the Web client. This can be disabled by the Admin or the User from their settings page

  NOTE: This was investigated further by the DPO team- This means the Host has the ability to screen share but others within the meeting do not without permission. This can be disabled by the Admin or the User from their settings page if required.

Join Before Host Emails Disabled

- Notifications sent to the host via email when participants are waiting for the host to join the meeting have been disabled.

Setting to Allow Participants to Rename Themselves

- Account admins and hosts can now disable the ability for participants to rename themselves in any meeting. This setting is available at the account, group, and user level in the Web portal.

Language for Directory and Company Directory (please note, this does not impact your account)

- Domain contacts: For free Basic and single licensed Pro accounts with unmanaged domains, contacts in the same domain will no longer be visible. We've also removed the option to auto-populate your Contacts list with users from the same domain. If you would like to keep those contacts, you can add them as External Contacts.

Change in visibility of contacts with same domain (please note, this does not impact your account)

- For Basic and single licensed Pro accounts with unmanaged domains, contacts in the same domain will no longer be visible under 'Company Directory' in the 'Contacts' tab. Consequently, for the single Pro accounts with unmanaged domains, we've removed the option in the admin experience to populate Company Directory with users from the same domain. If these affected users would like to keep contacts with the same domain, they can add them as External contacts. This change will not impact paid accounts with multiple licenses and all accounts with managed domains.

Please be sure to update to our latest release to take advantage of these new features. We also highly encourage you to register for our webinar to get an overview of this latest release, and subscribe to our Blog for more information and resources in the days to come.

Best,

Customer Success Advisory Team

Appendix B: 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 more easily?	Not investigated
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).	Not investigated
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?	US-EU Privacy Shield

Appendix C: Full DPIA for Zoom

Project Title	**Zoom Meeting**
Project Lead	**Kevin Flint - Headteacher**
Contact Details	**k.flint@morton.derbyshire.sch.uk**
DPO	**Jane Radford**
Contact Details	**Janer24@morton.derbyshire.sch.uk**
Date DPIA Completed	**4th May 2020**

General Project Description

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties:

Whilst the School is subject to the lockdown order issued by the UK Government is response to the Covid-19 outbreak, Zoom has been identified as a platform to necessitate the need to maintain regular meetings with key staff and Trustees in the most productive way possible.

It is only intended to be used during the period of lockdown and has been chosen because of the ease of use and the company offering premium services to the education sector for no fee until the lockdown is lifted.
If a VC facility is required post lockdown, then Zoom and other alternatives would be more rigorously investigated and be subject to a second DPIA.

Zoom offers a virtual meeting platform, in which a single registered user, can host a meeting for many attendees to join via invitation.

The private meeting allows all members to share a video feed, audio stream, text chat session, and desktop depending on the device being connected.

The platform only requires one user to be a registered member (Headteacher) who has control of the functionality available within the meeting for attendees (Such as recording and desktop share)

This account sets the restrictions for all participants of the meetings and has been pre-configured by the ICT team to remove additional features that are not needed, which in turn reduces the amount of data being processed by Zoom.

All attendees however need to be able to install the Zoom client on an internet connected device to join the meeting. Staff will be trained on how to do this.

The host can invite anybody to the meeting using an email address, it is not restricted to the School domain. The host must be careful when sending out invitations, and also once a meeting has begun to screen all attendees who join (use of 'waiting room').

Each meeting generates an additional PIN code (MFA), unique to the particular instance to mitigate uninvited users joining via brute force attack on meeting ID's.

The implementation of this project does not involve the processing of any new types of data. It represents a new platform for processing existing types of data.

Will the project/system involve the processing of personal data or special category (sensitive) personal data?

YES

1. Systematic Description of the Envisaged Processing Operations

1.1 Identify the data subjects:

Students Parents Contacts at other organisations Governors

1.2 What personal data will be processed?

Potentially all categories of personal data specified in all school Privacy Notices will be processed.

1.3 What special category (sensitive) data or criminal convictions data will be processed?

See 1.2 This includes all special category data which the school processes, as detailed in our Privacy Notices.

1.4 What are the purposes and lawful grounds for processing the personal data identified above?

Personal Data	Purpose	Lawful basis
See 1.2	No new data is being processed; personal data to be discussed over video conferencing suite i.e. Zoom, due to COVID-19 pandemic and inability for School to hold face to face meetings.	Public Task Duty

1.5 Describe the nature, scope and context of the processing, including a functional description of the processing operations:

Online video conferencing will take place. All attendees and host can broadcast a live video feed and audio stream. Host only can broadcast desktop presentations to all attendees. Only one user account for school (HT), but can invite 'guest' attendees by sending an email invite.

Nature and Purpose of Processing: Zoom will Process Personal Data on behalf of Customer for the purposes of providing the Services in accordance with the Agreement.

Duration of Processing: The term of the Agreement plus the period until Zoom deletes all Personal Data processed on behalf of Controller in accordance with the Agreement. Categories of Data Subjects: Individuals about whom Personal Data is provided to Zoom via the Services by (or at the direction of) Customer or Customer's end users, which may include without limitation Customer's employees, contractors and end users.

Type of Personal Data: Personal Data provided to Zoom via the Services by (or at the direction of) Customer or Customer's end users, including but not limited to the following:

User Profile: First Name, Last Name, Phone (optional), Email, Password (if SSO is not used), Profile Picture (optional), Department (optional)

Meeting Metadata: Topic, Description (optional), participant IP addresses, device/hardware information

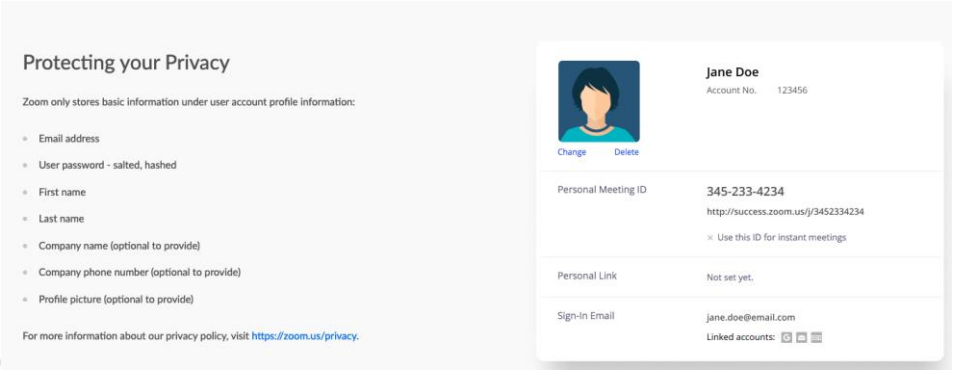
Cloud Recordings (optional): Mp4 of all video, audio and presentations, M4A of all Audio, Text file of all in meeting chats, Audio transcript file IM Chat Logs

1.6 Describe the assets on which the personal data relies (hardware, software, people, paper, networks, transmission channels)

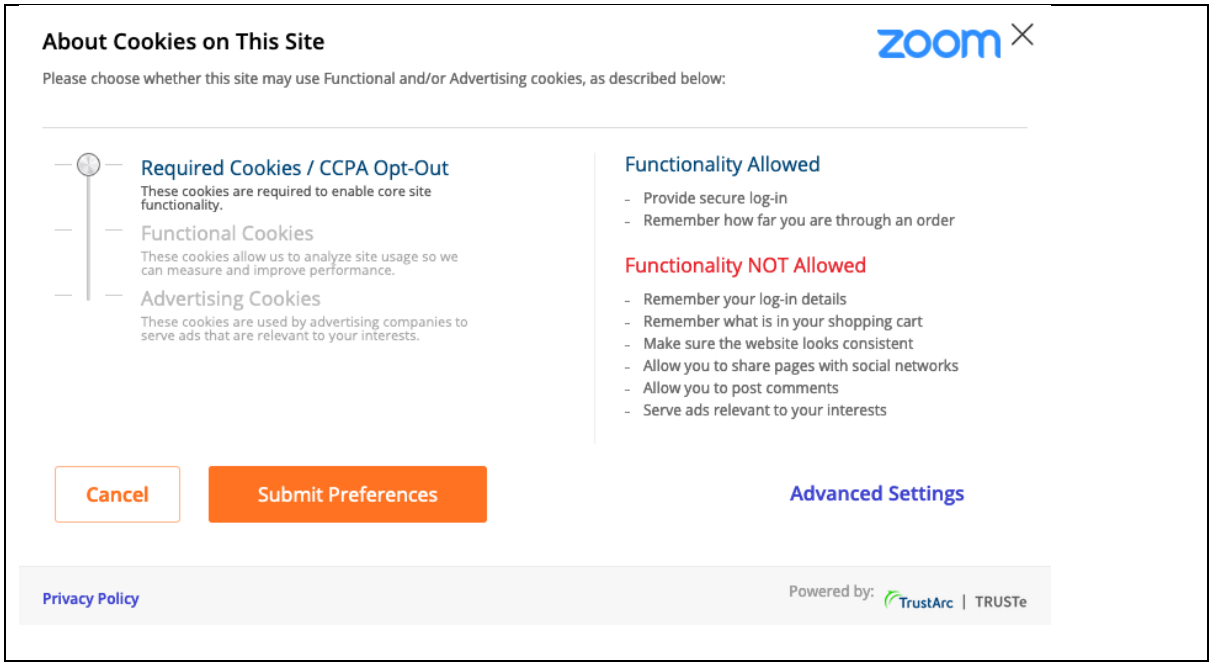
The internet
School IT staff
Teaching and admin staff
Internal/external Microphones / headsets
Laptops, desktops, tablets, phones. Some will be school property, others will be privately owned devices
Staff parent and pupil home Wi-Fi and internet providers

1.7 Set out the periods for retention of the personal data:

Zoom do not retain meetings once they have finished, unless an attendee initiated a recording, or saved the chat.
Zoom hold limited account holder data until the account is terminated. (Name, email address, company name)



Cookies on the HT account should be set to 'Required cookies/CCPA Opt-Out only



1.8 Set out details of any data sharing with third parties, including sub-processors:

https://zoom.us/subprocessors
Services for internal Sales, Support, PR, Billing, Infrastructure.
School will opt out of sale of personal information via the reduced cookie settings.

1.9 Set out details of any data sharing outside the EEA or with any international organisations:

The majority of the Zoom service is hosted in the United States, with additional technical and billing support in Malaysia, and payment management and fraud detection systems in Europe.

2. Necessity and Proportionality Assessment

2.1 If legitimate interest is identified as the lawful basis, set out details below:
Not applicable.

2.2 Identify any personal data processed in a manner which is not necessary for the identified purpose:

We will not process any data which on Zoom which is not already covered by school privacy notices. It is envisaged that no new data will be processed by this project. Recordings of video and audio calls will be disabled.
In recognition of the sensitivity around biometrics, the video calling features, ie live video footage of individuals, will not be used for identification purposes.

3. Assessment of Risks to the Rights and Freedoms of the Data Subjects

Consider and describe the risks to the rights and freedoms of the data subjects in the following areas:

3.1 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 School network shares will also apply to the same activity on Zoom. The school has identified Public Task as a lawful basis for the act of processing data on Zoom. This is because the school have a duty to educate/promote the welfare of students and continue to do so in the COVID-19 pandemic, albeit by video conference.

3.2 Fairness and transparency of processing

Moderate risk that staff use Zoom 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. DPO advises that Zoom is added to privacy notices as an addition to the COVID-19 situation.

3.3 Data minimisation

Low risk - Live video feeds and audio streams are being processed during a meeting, but this is not retained by Zoom once a meeting ends. Email address of the host will be retained for login purposes.

3.4 Maintaining accurate and up to date data

Low risk that the HT details will change and need to be changed in the hosting account.

3.5 Ability for data subjects to opt out or object to processing

We accept that it will not be possible for data subjects to opt out of having their basic data processed on Zoom, but have ensured where possible, additional processing has been opted out. Privacy Policy https://zoom.us/privacy No user is compelled to join a Zoom conference and they can raise objections to joining a meeting by contacting the host separately.

3.6 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 Zoom to be able to respond to an SAR.

3.7 Rights of the data subjects

Right to be informed: School to add Zoom to list of processors and inform parents this will be used via privacy notice Right to access: No recordings. Any data shared via screens should not contain personal data. Zoom will assist with a SAR where a valid request is received. No automated profiling Right to data portability is limited as the use of Zoom is not via consent or contract. Right to restrict processing: can be achieved by not utilising Zoom where data is inaccurate. School have administrative rights to amend login details where these may be incorrect.

Low risk of difficulty complying with Right to Rectification and Right to Erasure as only basic information is stored. Conversations will not be recorded and the only recordable information will be the host's email address, which can be updated as and when required.

Zoom have stated in their DPA:
8.1 Zoom shall, to the extent permitted by Applicable Data Protection Law, promptly notify Customer upon receipt of a request by a Data Subject to access, rectify, restrict, erase, transfer, or cease Processing, withdrawal of consent to Processing, and/or objection to being subject to Processing that constitutes automated decision-making (such requests individually and collectively "Data Subject Request(s)"). If Zoom receives a Data Subject Request in relation to Customer's data, Zoom will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Services. For the avoidance of doubt, Zoom shall not be obligated to grant a Data Subject Request where the Data Subject is not entitled to the relief sought.

8.2 Zoom shall, at the request of the Customer, and taking into account the nature of the Processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Customer in complying with Zoom DPA, December 2019 6 any Customer obligation under Applicable Data Protection Law to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, provided that (i) Customer is itself unable to respond without Zoom's assistance and (ii) Zoom is able to do so in accordance with all applicable laws, rules, and regulations. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Zoom.

3.8 Transfers to third parties

Low risk that staff might accidentally share personal data with another individual or organisation.

Zoom uses US hosted suprocessors listed here: https://zoom.us/subprocessors

3.9 Transfers outside the EEA or to international organisations

Medium risk as personal data is stored outside the EEA. However, Zoom is certified under the EU-US Privacy shield.

Data processing agreement here :
https://zoom.us/docs/doc/Zoom_GLOBAL_DPA_December_19.pdf

Low risk that a sub processor engaged by Zoom will access our data from overseas in a manner which is not compliant with GDPR- see DPA above.

3.10 Retention and deletion

Medium risk that the school will struggle to identify and delete all personal information held on Zoom at the end of its retention period. This will be reviewed no later than 6 months notwithstanding the requirement to review this DPIA when schools return to normal processing.

3.11 Data security

Low risk that an attendee might share personal data with the wrong person in error.
Zoom have offered guidance regarding screen sharing here:
https://support.zoom.us/hc/en-us/articles/360041591671?zcid=1231

Zoom information:

- On April 1, we:
  - Published a blog to clarify the facts around encryption on our platform – acknowledging and apologizing for the confusion.
  - Permanently removed the attendee attention tracker feature. *(updated 4/2 to clarify that it's permanently removed)*
  - Released fixes for both Mac-related issues raised by Patrick Wardle.
  - Released a fix for the UNC link issue.
  - Permanently removed the LinkedIn Sales Navigator app after identifying unnecessary data disclosure by the feature. *(updated 4/2 to clarify that it's permanently removed)*

Also see email of 9/4/20 from Zoom setting out further changes that have been made to security.

Zoom Data Processing Agreement:

6.2 Zoom shall implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:
6.2.1 the pseudonymisation and encryption of personal data;
6.2.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
6.2.3 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
6.2.4 a process for regularly testing, assessing and evaluating the effectiveness of security measures.

3.12 Further risks

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.

Medium risk of issues if staff use Zoom video conferencing facilities for non-work purposes whilst at home.

Low risk that a data breach occurs because staff are not sufficiently trained and familiar with Zoom to be able to correctly configure all features for optimum privacy.

4. Measures Envisaged to Address the Risks

4.1 Complete the following table using the risks identified above:

Identified risk in paragraph 3 above	Risk	Controls to be implemented	Proposed Mitigation
3.1	No new data is being generated or processed by	HT to control who is in attendance, the agenda for the meetings, and to host	Lowers risk

	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 Zoom. The school has identified Public Task as a lawful basis for the act of processing data on Zoom.	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.	
3.2	Low risk that attendees use Zoom 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 filesharing, and chat. HT only to share relevant presentations, and to keep meetings focused on agenda.	Lowers risk
3.3	Low risk - Live video feeds and audio streams are being processed during a meeting, but this is not retained by Zoom 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
3.4	Low risk that the HT details will change and need to be changed in the hosting account.	Zoom hold limited personal data for account holder – If HT details change in the lockdown period, account will need to be deleted. This is possible and Zoom will permanently delete accounts once they have been deleted by the user.	Lowers risk
3.5	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 Zoom, but have ensured where possible, additional processing has been opted out. Privacy Policy https://zoom.us/privacy Host will invite attendees to Zoom meetings via email. ICT team will have a trail of all invites sent out and can request Zoom delete and stored meta data. Meeting Metadata: Topic, Description (optional), participant IP addresses, device/hardware information To make a request, please contact our Privacy Team at privacy@zoom.us	Lowers risk

		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. This will mean the school may have to consider whether an alternative platform can be utilised for VCs. School has an alternative platform available for this scenario.	
3.6	Moderate risk that ICT admin staff will not be able to locate all relevant personal information stored on Zoom to be able to respond to an SAR.	We have to request any information from Zoom as we have no access to this. To make a request, please contact our Privacy Team at privacy@zoom.us Access: You can request more information about the personal data we hold about you. You can request a copy of the personal data.	Lowers risk
3.7	Low risk of difficulty complying with Right to Rectification and Right to Erasure as only basic information is stored.	From Privacy policy - https://zoom.us/privacy Erasure**:** You can request that we erase some or all of your personal data from our systems. For instructions on how to delete your account please see https://support.zoom.us/hc/en-us/articles/201363243-How-Do-I-Delete-Terminate-My-Account Zoom DPA also includes: Following completion of the Services, at Customer's choice, Zoom shall return or delete the Personal Data, except as required to be retained by law, rule or regulation that is binding upon Zoom or, if the Personal Data is in the possession of an Authorized Subprocessor or Subprocessors, as required to be retained by an Authorized Subprocessor by law, rule or regulation that is binding upon the Subprocessor. If return or destruction is impracticable or prohibited by law, rule or regulation, Zoom shall take measures to block such Personal Data from any further Processing (except to the extent necessary for its continued hosting or Processing required by law, rule or regulation) and shall continue to	Lowers risk

		appropriately protect the Personal Data remaining in its possession, custody, or control and, where any Authorized Subprocessor continues to possess Personal Data, require the Authorized Subprocessor to take the same measures that would be required of Zoom. If Customer and Zoom have entered into Standard Contractual Clauses as described in Section 7 (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 Zoom to Customer only upon Customer's request.	
3.8	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. Zoom now have a default position that invitees must attend a meeting by utilising a password within the invite link. The host will then have to allow the invitee into the conference from the virtual waiting room. Disable join before host. This gives the host greater ability to ensure those attendees are legitimately invited to the meeting and prevent 'Zoombombing'. The host can lock the session after attendees have entered to prevent further access. Zoom have stated: in a meeting where all of the participants are using Zoom clients, and the meeting is not being recorded, we encrypt all video, audio, screen sharing, and chat content at the sending client, and do not decrypt it at any point before it reaches the receiving clients.	Lowers risk
3.9.1	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 is held outside of the EU, as is meta data from meeting attendees. Zoom use the EU-US Privacy Shield framework to provide mechanism to comply with GDPR requirements. Zoom DPA: Any transfer of Personal Data made subject to this Addendum from member states of the European Union, Iceland,	Lowers risk.

		Liechtenstein, Norway, Switzerland or the United Kingdom to any countries which do not ensure an adequate level of data protection within the meaning of the laws and regulations of these countries shall, to the extent such transfer is subject to such laws and regulations, be undertaken by Zoom through one of the following mechanisms: (i) in accordance with the Swiss-U.S. and EU-U.S. Privacy Shield Framework and Principles issued by the U.S. Department of Commerce, both available at https://www.privacyshield.gov/EU-US-Framework (the "Privacy Shield Principles") or (ii) the Standard Contractual Clauses set forth in Exhibit C to this Addendum. 7.2 2 If transfers are made pursuant to 7.1(i), Zoom self-certifies to, and complies with, the Swiss-U.S. and EU-U.S. Privacy Shield Frameworks, as administered by the U.S. Department of Commerce, and shall maintain such self-certification and compliance with respect to the Processing of Personal Data transferred from member states of the European Union.	
3.9.2	Low risk that a sub processor engaged by Zoom will access our data from overseas in a manner which is not compliant with GDPR	School have opted out where possible of sharing meta data with third parties. Zoom will need to continue to utilise sub-processors in order to provide the service, but have stated in their DPA: 5.3 Zoom shall ensure that all Authorized Subprocessors have executed confidentiality agreements that prevent them from disclosing or otherwise Processing, both during and after their engagement by Zoom, any Personal Data both during and after their engagement with Zoom. 5.4 Zoom shall, by way of contract or other legal act under applicable law ensure that every Authorized Subprocessor is subject to obligations regarding the Processing of Personal Data that are no less protective than those to which the Zoom is subject under this Addendum. Zoom shall, exercising reasonable care, evaluate an	Lowers risk.

		organization's data protection practices before allowing the organization to act as an Authorized Subprocessor. 5.5 Zoom shall be liable to Customer for the acts and omissions of Authorized Subprocessors to the same extent that Zoom would itself be liable under this Addendum had it conducted such acts or omissions.	
3.10	Medium risk that the school will struggle to identify and delete all personal information held on Zoom 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. See clause 7 for Zoom contractual stance.	Lowers risk
3.11	Low risk that an attendee might share personal data with the wrong person in error.	Host to screen all attendees before meeting commences. See clause 8 for Zoom default position.	Lowers risk
3.12.1	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.	Lowers risk.
3.12.2	Medium risk of issues if staff use Zoom 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.
3.12.3	Low risk that a data breach occurs because ICT admin staff are not sufficiently trained and familiar with Zoom to be able to correctly configure all features for optimum privacy.	ICT team 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 Zoom is included here: and shared with staff who will have access to the service.	Lowers risk.

5. Compliance with Guidance/Codes of Conduct

5.1 Identify any applicable guidance and/or codes of conduct issued by the Government, the ICO, the Commission or any relevant association or body:

NA

5.2 Where applicable, set out details of compliance with any relevant guidance and/or code of conduct:

EU-US Privacy Shield

6. Involvement of Data Subjects

6.1 Where appropriate, seek the views of the data subjects or their representatives on the intended processing and set out the findings below:

Not appropriate to seek data subject views as the processing enables the school to carry out their duties as an authority under the lawful basis of public task.

6.2 If the views of the data subjects have not been sought, set out the rationale below, with reference to any commercial or public interests and the security of processing operations:

The School is carrying out its Public Task duties. This DPIA is being conducted during a period of school closure and national lockdown due to COVID-19. Zoom will help the School fulfil its obligations at this time.

7. DPIA Review

7.1 Identify any planned changes to the project or system and set a date to review this DPIA:

Level two of rolling out a VC service will commence post lockdown if the School decide the functionality has significant benefit over what is already available to staff using Microsoft Teams. The School commits to carrying out a fresh DPIA as part of the Level two project.

7.2 This DPIA will be reviewed to assess if processing is performed in accordance with this DPIA 6 months from the date of completion or, alternatively,: one year.

8. Approval

This project was assessed and its Data Protection Impact Assessment approved:

The DPO has advised that the use of Zoom should be restricted in as far as is possible. There are a number of issues that have been flagged, such as Zoombombing and forcing staff to use Zoom when there is alternative provisions available. The school have accepted the risks despite and wish to continue with the application of Zoom.

School DPO	Clare Wilson Data Protection Consultant M: 07971 373630 T: 01629 538555 clare.wilson@derbyshire.gov.uk
Head Teacher/Governor	Kevin Flint

Reviewed and approved May 2020

Acknowledgements:
With many thanks to Tony Sheppard, GDPR in Schools and Jessica Sweet, DPO, Coventry City Council for their contribution to this document.