

The Active Learning Trust

DATA PROTECTION IMPACT ASSESSMENT FORM

ZOOM

Identify the need for a DPIA

Explain what the project or process aims to achieve; what benefits will be to the Academy, to individuals and other parties and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why the need for DPIA was identified.

Zoom Video Conferencing Inc created a videoconferencing service – “Zoom” for corporate webinars and meetings and has become a forum for nearly every kind of social function, including school/ home based learning classes during the coronavirus pandemic.

A DPIA is required as special category data could be shared by students.

Describe the nature & scope of the processing:

What and whose personal data is required and does it include special category or criminal offence data? How will you collect, use, store and delete data? What is the source of the data? Will you share the personal data with anyone? Will personal data be manually input or feed direct from SIMs? How many individuals are affected?

Any personal data including special category of personal data that a school/ pupil wishes to share will be heard/seen by others in the video conference.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

A number of security and privacy flaws have been identified and Zoom has undertaken measures to identify and quickly patch vulnerabilities. It formed an advisory council of chief security officers from other companies and hired Alex Stamos, Facebook’s former chief security officer, as an advisor.

Security and Privacy Issues identified and corrected

(1) Personal Zoom videos were left viewable on the open web, including one-on-one therapy sessions and school classes.

Action:

A virtual waiting room is now set automatically. This allows students who want to join a class to be held in a virtual waiting room before being let into the classroom. This allows a teacher to check who each person is before allowing them entry. There is also a setting to allow known students to skip the waiting room so teachers don't have to manually allow 30 pupils every time. This means that uninvited people can not gain access to a video.

(2) Zoom marketed its video conferencing service as protected by end-to-end encryption meaning that an intermediary, include Zoom itself, cannot intercept and decrypt users' communications as it moves between the sender and receiver. However it had transport encryption, which enables the company to decode the content of calls. That means the company could hypothetically be susceptible to pressure from government authorities to disclose communications.

Action:

Zoom's video conferencing service is now end to end encrypted – refer [Zoom Encryption](#):

- All customer data transmitted from a client to the Zoom cloud is encrypted in transit using one of the following methods – HTTPS, AES-256 in ECM mode, SRTP
- All customer data transmitted from a web browser to the Zoom cloud (including on their website and web meeting client is encrypted in transit using one of the following methods – TLS 1.2, AES-256.

However when using a third party device – customer data transmitted via these devices may not be encrypted in transit to and from the Zoom's system. Once the data reaches the Zoom system it is encrypted at that point.

3) Zoom's default setting allowed anyone to join video calls if they had the meeting ID, which is a number [9 to 11 digits](#) long. These meeting IDs are easy to guess — with an automated tool ([called "war-dialing"](#)), anyone could access thousands of meetings within a day by simply making a lot of guesses.

Action:

Teachers can now generate a new ID for every meeting launched using the options panel, instead of using their personal meeting ID.

Teachers can now change the settings to ensure students need a password to access the meeting.

(4) "Zoombombing" is when uninvited participants interrupt or derail a meeting. Sometimes it's harmless trolling, but often it rises to the level of harassment. Schools have reported getting Zoombombed with racist taunts and pornographic images.

Action:

Students who are joining a session manually are required to enter the password provided by the meeting host. People who received an invitation will also still be able to join just by clicking the link.

(5) Zoom's app for iPhones sent data about users' devices to Facebook, including about users who did not have Facebook accounts. The company was hit with at least [two lawsuits](#) in federal court, one by a California resident [who alleges](#) Zoom violated the state's

new Consumer Privacy Act by disclosing information to Facebook without providing consumers with adequate notice or the ability to opt out.

Action: Zoom Chief Executive Eric Yuan said in a [blog post March 27](#) that the company removed code that sent user data to Facebook in an updated version of the iOS app. The company [updated its privacy policy](#) March 29.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

To allow teachers to video conference lessons with students.

Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

N/A

Assess necessity and proportionality

Describe compliance and proportionality measures.

What is the lawful basis for processing	6.1.(e) task carried out in the public interest If special category data is shared – 9.2(g) substantial public interest.
Does the processing actually determine the school's purpose?	Yes.
Is there another way to achieve the same outcome?	No as children are now at home due to the Pandemic.
How will you prevent function creep?	The system is purely a video conferencing service.
How will you ensure data quality and data minimisation	The personal data uploaded by a teacher/student.
What information will you give individuals?	Privacy Notices are held on a school's website.
How will you help to support their rights?	Rights on personal data usage are covered in the Trust's SAR Policy and various privacy notices.

What measures do you take to ensure processors comply?	Processors will be audited – compliance with Article 28.3.
How do you safeguard any international transfers?	<p>Zoom Video Communication, Inc. participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield. Zoom so personal data may be held in the US – this meets the ICO’s data privacy requirements.</p> <p>Schools may choose to have their data stored outside of the U.S; for example, they may choose to have their data stored in their geographic vicinity. It may store local data locally in order to comply with specific local laws and regulations.</p>

Identify and assess risks

For each of the following risks – identify the likelihood of harm (remote, possible or probable); severity of harm (minimal, significant or severe) and overall risk (low, medium or high)

Risk	Answer and likelihood/severity of harm and overall risk
1. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.	
1.1 The purpose of the project/process has not been identified.	Remote likelihood of harm, minimal severity of harm and overall low risk as the purpose of the software is to provide a video conferencing service.
1.2 The lawful basis for processing has not been established.	Remote likelihood of harm, minimal severity of harm and overall low risk as the lawful basis for processing personal data has been established.
1.3 Individuals have not been told about the use of their personal data.	Remote likelihood of harm, minimal severity of harm and overall low risk as schools record how personal data of pupils is used within their privacy notices.
1.4 The rights of individuals are unknown.	Remote likelihood of harm, minimal severity of harm and overall low risk as the rights of pupils are recorded in schools’ privacy notices and in the Trust’s Subject Access Request Policy.
1.5 If consent is required, its collection, withholding and withdrawal have not been identified.	Remote likelihood of harm, minimal severity of harm and overall low risk as consent is not required.
1.6 Personal data may be held outside the EEA?	Remote likelihood of harm, minimal severity of harm and overall low risk as Zoom’s Privacy Policy records that its services generally store data in the United States, though through its global data

	<p>centres, data may come in from wherever users are located.</p> <p>It may transfer personal data to the U.S., or to third parties acting on their behalf, for the purposes of processing or storage.</p> <p>Customers may choose to have their data stored outside of the U.S; for example, they may choose to have their data stored in their geographic vicinity. It may store local data locally in order to comply with specific local laws and regulations.</p> <p>By using Zoom, or providing personal data for any of the purposes stated above, a user consents to the transfer to and storage of personal data in the U.S., or other location as directed by the customer.</p> <p>In certain limited circumstances, courts, law enforcement agencies, regulatory agencies, or security authorities in those other countries may be entitled to access personal data.</p>
<p>1.7 Privacy notices require amendment but haven't been amended</p>	<p>Remote likelihood of harm, minimal severity of harm and overall low risk as Privacy Notices do not requirement amendment.</p>
<p>1.8 Personal information will be passed to third parties and sub processors.</p>	<p>Remote likelihood of harm, minimal severity of harm and overall low risk as although the Privacy Policy records that it uses third-party service providers to help provide portions of the Zoom services and give support it requires service providers to use data only in order to perform the services that Zoom has hired them to do (unless otherwise required by law).</p> <p>For example, it may use a company to help us provide customer support. The information they may receive as part of providing that support cannot be used by them for anything else – e.g. public cloud storage vendors, carriers, our payment processor, and its service provider for managing customer support tickets.</p> <p>They only receive data needed to provide their services to Zoom which has agreements with such service providers that say they cannot use any of this data for their own purposes or for the purposes of another third party.</p> <p>Zoom prohibits its service providers from selling data they receive from Zoom or receive on Zoom's behalf.</p>
<p>1.9 There is no data sharing agreement, protocol or contract</p>	<p>Remote likelihood of harm, minimal severity of harm and overall low risk as there are terms and conditions of usage.</p>

2. Personal data shall be collected for specified, explicit and legitimate purposes	
2.1 The project does not cover all of the purposes for processing personal data.	Remote likelihood of harm, minimal severity of harm and overall low risk as the project covers all the purposes for processing personal data.
2.2 Potential new purposes have not been identified as the scope of the project expands.	Remote likelihood of harm, minimal severity of harm and overall low risk as the software is unlikely to be used for another purpose.
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed?	
3.1 The information is not of good enough quality for the purposes it will be used.	Remote likelihood of harm, minimal severity of harm and overall low risk as the information comes directly from a teacher/student.
4. Which data could not be used without compromising the needs of the project?	
4.1 Personal data is not accurate and not kept up to date	Remote likelihood of harm, minimal severity of harm and overall low risk.
4.2 Any new software or process does not allow the amendment of data when necessary.	Remote likelihood of harm, minimal severity of harm and overall low risk as personal data can be amended.
4.3 The Academy does not ensure the accuracy of data obtained from individuals or other organisations.	Remote likelihood of harm, minimal severity of harm and overall low risk as no data is provided by other individuals or other organisations.
5. Personal data shall be kept in a form which permits identification if data subjects for no longer than is necessary	
5.1 The retention period is not suitable for the personal data being processed.	Remote likelihood of harm, minimal severity of harm and overall low risk as the Privacy Policy records that it does not monitor meetings or even store them after a meeting is done unless they are requested to record and store them by the meeting host. Zoom alerts participants via both audio and video when they join meetings if the host is recording a meeting, and participants have the option to leave the meeting. When the meeting is recorded, it is, at the host's choice, stored either locally on the host's machine or in the Zoom cloud. Customers can delete their content at any time.
5.2 The procured system will not allow deletion of information in line with retention periods.	Remote likelihood of harm, minimal severity of harm and overall low risk as the Trust does not have a set retention period for such video conferencing.
6. Personal data shall be processed in a manner that ensures appropriate security of the personal data.	

<p>6.1 The new system(s) does not provide protection against any identified security risks.</p>	<p>Possible likelihood of harm, minimal severity of harm and overall medium risk as on 2 April 2020 the CEO of Zoom confirmed over the next 90 days it plans to:</p> <ul style="list-style-type: none"> ▪ freeze development of new features to focus on safety and privacy • conduct a review with independent experts to understand new security features needed for new customers • prepare a transparency report on data requests • enhance its bug bounty program • hold a weekly webinar to provide privacy and security updates <p><u>Link to BBC News article</u></p>
<p>6.2 Training and instructions will not be given to staff to operate new systems and keep data secure.</p>	<p>Remote likelihood of harm, minimal severity of harm and overall low risk as the Privacy Policy records that staff will be trained.</p>
<p>6.3 Where personal data is held outside the EEA, the security of such meets the ICO's requirements.</p>	<p>Remote likelihood of harm, minimal severity of harm and overall low risk as Zoom Video Communication, Inc. participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield. Zoom</p>

Identify measures to reduce risk


Identify additional measures that could be taken to reduce or eliminate risks identified as medium or high risk above.

Risk	Options to reduce or eliminate risk. Effect on risk (eliminated reduced accepted); residual risk (low, medium, high); measure approved – yes/no
<p>1. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.</p>	
<p>1.1 The purpose of the project/process has not been identified.</p>	<p>N/A as not high or medium risk.</p>
<p>1.2 Conditions for processing have not been established.</p>	<p>N/A as not high or medium risk.</p>
<p>1.3 Individuals have not been told about the use of their personal data.</p>	<p>N/A as not high or medium risk.</p>

1.4 The rights of individuals are unknown.	N/A as not high or medium risk.
1.5 If consent is required, its collection, withholding and withdrawal have not been identified.	N/A as not high or medium risk.
1.6 Personal data may be held outside the EEA?	N/A as not high or medium risk.
1.7 Privacy notices require amendment but haven't been amended	N/A as not high or medium risk.
1.8 Personal information will be passed to third parties and sub processors.	N/A as not high or medium risk.
1.9 The us no data sharing agreement, protocol or contract	N/A as not high or medium risk.
2. Personal data shall be collected for specified, explicit and legitimate purposes	
2.1 The project does not cover all of the purposes for processing personal data.	N/A as not high or medium risk.
2.2 Potential new purposes have not been identified as the scope of the project expands.	N/A as not high or medium risk.
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed?	
3.1 The information is not of good enough quality for the purposes it will be used.	N/A as not high or medium risk.
4. Which data could not be used without compromising the needs of the project?	
4.1 Personal data is not accurate and not kept up to date	N/A as not high or medium risk.
4.2 Any new software or process does not allow the amendment of data when necessary.	N/A as not high or medium risk.
4.3 The Academy does not ensure the accuracy of data obtained from individuals or other organisations.	N/A as not high or medium risk.

5. Personal data shall be kept in a form which permits identification if data subjects for no longer than is necessary	
5.1 The retention period is not suitable for the personal data being processed.	N/A as not high or medium risk.
5.2 The procured system will not allow deletion of information in line with retention periods.	N/A as not high or medium risk.
6. Personal data shall be processed in a manner that ensures appropriate security of the personal data.	
6.1 The new system(s) does not provide protection against any identified security risks.	Much work has been undertaken to correct and close data privacy issues. The company now has a 90 day action plan. I am however aware that schools in the UK use this software and can be contacted if we have any concerns.
6.2 Training and instructions will not be given to staff to operate new systems and keep data secure.	N/A as not high or medium risk.
6.3 Where personal data is held outside the EEA, the security of such meets the ICO's requirements.	N/A as not high or medium risk.

Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	C Driver, DPO 20/4/20	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	n/a	If accepting any residual high risk, consult the ICO before going ahead
Summary of DPO advice – Zoom is GDPR compliant – however please ensure the actions recorded below are undertaken to ensure privacy of personal data.		
Second Signature – Director of Finance and Operations:	 20 April 2020	
This DPIA will kept under review by:	Six months given the 90 day action plan.	The DPO should also review ongoing compliance with DPIA

Integrate the DPIA outcomes into the project plan

This step records the DPIA outcomes that need to be integrated into the project plan and the names of persons responsible for such work.

Actions to be taken	Date for completion of actions	By whom
Choose to have data stored in the EU – this means that privacy notices will not require amendment.	During setting up of account	Teacher
A teacher to generate a new ID for every meeting launched using the options panel, instead of using their personal meeting ID.	During setting up of account	Teacher
A teacher to change the settings to ensure students need a password to access the meeting.	During setting up of account	Teacher
Teachers to lock a classroom once a class has started and all students have arrived so that no one else can join.	During setting up of account	Teacher
Make sure students don't take control of the screen. Prevent them from sharing random content by limiting screen sharing so only the teacher can present to the class.	During setting up of account	Teacher
Prevent private messaging amongst students so they can't talk to one another without a teacher's knowledge.	During setting up of account	Teacher
Teachers to turn a student's video off if a student provides unwanted, distracting, or inappropriate gestures on video.	During setting up of account	Teacher
Teachers to block unwanted, distracting or inappropriate noise from students by muting them. Teachers can also enable "mute upon entry" in their settings.	During setting up of account	Teacher

<p><u>Turn off file transfer</u> In-meeting file transfer allows people to share files through the chat. Toggle this off to keep the chat from getting bombarded with unsolicited content.</p>	During setting up of account	Teacher
<p>Zoom provides a pop-up notification when there is a new mandatory or optional update within 24 hours of logging in – please make sure IT is aware of and uploads such updates so that any patches Zoom makes to security vulnerabilities are added to your device.</p>	When ever a notification is received.	Teacher/ICT
<p>The background behind a student will provide insight into people's private spaces. Need to consider this when asking students to video link. Request that students upload one of Zoom's default backgrounds. You Tube Link - Link</p>	During setting up of account	Teacher/ Student
<p>Opt Out of “Sales”: Ask Zoom to take a teacher out of certain advertising related to your personal data by clicking on the “Do Not ‘Sell’ My Personal Information” link.</p>	During setting up of account	Teacher
<p>Diarise to delete video meetings or delete account if not longer required: Link</p>	End of summer term	Teacher