MAY 2020

Zoom Video Conferencing: Protocols, Permissions, Risk Assessment and Privacy Impact Assessment

COVID19 Response

DHOON / LAXEY FEDERATION
DEPARTMENT OF EDUCATION, SPORT AND CULTURE

Monday 25th May 2020

Dear parents and carers

Zoom Video Conferencing – Protocols and Permissions

We have been looking at ways to provide a video conference and chat opportunity for pupils. We have looked at Microsoft Teams and Zoom.

We feel that Zoom has the most user-friendly options that will allow children to see each other and their teacher. As with all new platforms we are required to explore any potential data risks and access issues. We have complied a Risk Assessment and Privacy Impact Statement, which is attached to this letter, and is available on our school websites. Please read these, as by providing them we consider that all relevant information – including risks – have been explicitly shared.

To minimise any potential issues we have completed a protocol for meetings which is set out below:

⇒ Children / parents will only need a browser and do not need to download any applications.
⇒ All meetings will be hosted by Mr Kelly or a member of the teaching staff in the Federation.
⇒ Invitations will be sent to the children's parental email address to join a planned meeting.
⇒ All invites to the meeting contain a website address (URL) and a password.
⇒ To access the meeting the address is copied and pasted into a browser such as Chrome or Safari.
⇒ The invited person will gain entrance to a waiting room and can only be admitted by the meeting organiser or teacher.
⇒ At the end of the meeting the organiser or teacher will end the meeting for everyone.
⇒ The teacher can control the mute buttons of each child during the meeting.
⇒ All participants will be muted on arrival. The meeting host will be able to control who speaks and when.
⇒ The meeting will be terminated as quickly as possible by the meeting host should it become apparent that it has been "zoombombed" or accessed by someone who should not have been present.

As the educational landscape continues to change and develop in the face of the COVID19 global pandemic, our response to delivering learning must continue to evolve. We have already been providing content for remote learning via our websites, instigated telephone communication and moved to provide ongoing direct access to our teaching staff through new email accounts. Our next step is to explore video conference opportunities for occasional remote delivery in real time.

We intend to hold one initial test meeting for all pupils on Friday 29th May at 10.30am and depending on the success of this, we may look to schedule additional meetings for smaller groups going forward.

Our initial meeting will be styled as a "Big School Assembly" and aims to bring together as many of our pupils as possible. The assembly will include a message from me, a chance to hear from some of the teachers, and one or two surprises that we hope to have in place.

For this first meeting, children will be muted on entry, and I will control who can speak and when. This level of control, which is achievable in Zoom, will help with the management of such a large conference. Obviously the children will need access to a device that allows them to switch on a video so that they can be seen on the conference screen – it will be lovely to see everyone's face in real time – but there is an opportunity for families to gather at webcams so mums, dads and carers can be part of the experience too. This is actually very important, because if we take this further with future meetings, then parents will have a clearer understanding of how the facility will work.

We need parental permission for your child to take part in these sessions, including the Big School Assembly on Friday. We won't assume you are happy for your child to take part, and you will only receive an invite if we have your express consent.

If parents are happy for their children to be included please can you reply with the following note or something similar to our LaxeyEnquiries@sch.im or DhoonEnquiries@sch.im email address.

"I agree that my child can take part in Zoom meetings scheduled by school and I confirm my child may be invited to sessions arranged by the school."

We will be able to accept email replies as confirmation of your agreement to our protocol, privacy impact statement and risk assessment.

The invite will be sent out on the morning of the assembly, in advance of 10.30am, and it will be delivered to the parental email address that we hold on record.

I hope to see as many of you as possible on Friday morning, and we will all have to keep our fingers crossed that the technology works. The staff have trialled Zoom for some of our staff meetings, and we can get it to work, but this is our first attempt at marrying it up with parental consents, a large number of invites and a wide audience. So please bear with us if there are teething issues and glitches.

Best wishes

Mr M Kelly
Executive Headteacher

RISK ASSESSMENT FORM – USING ZOOM TO DELIVER VIDEO-CONFERENCING IN REAL TIME WITH GROUPS OF PUPILS

Risk Classification
Likelihood (L): remote = 1 possible = 2 probable = 3
Severity (S): minor = 1 serious = 2 severe/fatal = 3
Risk Rating (LxS): low = 1-2 medium = 3-5 high = 6-9

Person making assessment: **M Kelly**		Date 22.05.2020				Review date: Ongoing	
Location or Activity Element	**Potential Hazard Description**	**Risk Classification**			**Action taken to reduce or control risk**	**Residual risk and further action req'd**	**Action (initial)**
		Likelihood	Severity	Rating			
Video conference session between pupils and a member of staff	Pupils sharing inappropriate content	2	2	4	Parents' permission requested and received. Parents can monitor session (and are actively encouraged to can sit in on the session.) All meetings scheduled by Dhoon/Laxey staff will use the waiting room feature that prevents users from entering the meeting without first being admitted by the host. Unique meeting ID used. Once everyone has joined the meeting or after 5 minutes of the session starting, we can 'Lock' the meeting so that nobody else can join. Each meeting hosted by a member of staff will be password protected. This password will be issued by email a short time before each scheduled meeting. First name of the child participating is correct before joining a session. All microphones will be muted on entry to the meeting. Pupils not to unmute unless asked to do so or the host does it for them. Each meeting will be scheduled for a specific time and will usually last no more than 30 minutes.	If anything inappropriate occurs during a meeting, the meeting will be stopped immediately. Chat feature closed by host – this needs to be set on the app not desktop. No screen sharing allowed. Check once sessions starts that an adult is present in the room.	

Video conference sessions other than with a member of staff	Pupils accepting conference invitations at other times with people purporting to be a member of staff	2	2	4	Routine & protocol established and shared with parents and children. Meetings scheduled will be advised in advance with set dates and times. Passwords also set and shared a short time before each session. Parents & children advised not accept any invitations to sessions at other times from people purporting to be a member of staff from Dhoon / Laxey Federation.		
Video conference session with pupils whose patents have not given permission	Leaked link to conference to children whose parents have not given permission for joining sessions	2	2	4	Date and time of chat only shared in secure email to parents who have expressed permission. This will be recorded in the Laxey/Dhoon information management system known as Arbor. Link to chat only shared in secure email to parents who have given permission Staff set up meeting. Laxey / Dhoon Zoom account will be used linked to school's professional email address.		
Video conference session between staff only	Confidential discussion about pupils or staff issues	2	2	4	Staff to join conference in a private space out of ear shot of non-Federation staff		
Video conference session between staff only	Leaked link to conference to others	2	2	4	All meetings scheduled by Executive Headteacher or staff will use the waiting room feature that prevents users from entering the meeting without first being admitted by the host. Unique meeting ID used Password issued to staff only & sent in advance. All microphones will be muted on entry to the meeting.		
Video conference session between staff only	Staff accepting conference invitations at other times with people purporting to be a member of staff	2	2	4	Routine & protocol established and shared with staff. Meetings scheduled will be advised in advance with set dates and times. Passwords also set and shared before session.	If anything inappropriate occurs during a meeting, the meeting will be stopped immediately.	

PRIVACY IMPACT ASSESSMENT - USING ZOOM TO DELIVER VIDEO-CONFERENCING IN REAL TIME WITH PUPILS

School/ Division/Team:	**DHOON/LAXEY FEDERATION**
Project Title:	**Zoom**
Lead/Contact Officer:	**EXECUTIVE HEADTEACHER**

Privacy Impact Assessment? (PIA) – pre-screening questions:

(These questions are intended to help you decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise.

[You can expand on your answers as the project develops if you need to. You can adapt these questions to develop a screening method that fits more closely with the types of project you are likely to assess].

Questions:	**Yes / No**
Will the project involve the collection of new information about individuals?	**Y**
Will the project compel individuals to provide information about themselves?	**Y**
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	**Y**
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	**Y**
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.	**N**
Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	**N**
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.	**N**
Will the project require you to contact individuals in ways that they may find intrusive?	**N**

Privacy Impact Assessment

Step one: Identify the need for a PIA

Explain what the project aims to achieve:	Implement Zoom based learning using break out sessions and meetings for online sessions including remote assemblies.
Benefits to the organisation:	Allows direct contact with data subjects – children, young people and students.
Benefits to individuals:	Continuation of the learning experience.
Benefits to other parties:	Educational development continues/
Other relevant documents related to the project:	https://www.privacyshield.gov/participant?id=a2zt0000000TNkCAAW&status=Active https://zoom.us/privacy Risk assessment and other documents provided by Dhoon/Laxey Executive Headteacher – to be amended as needed. Generic versions attached at the appendix Info relating to Zoom:

Type of Data	**Examples**	**Zoom Uses it to**
Information that identifies you	For customers: Account owner name, billing name and address, payment method	Create a customer account

	Your name, username and email address, or phone number, when you use this information to access or use our services The phone number a Zoom Phone user dials	Provide Zoom services Communicate with a customer Respond to requests for support
Other account data	Your phone number (if you choose to put it in), language preference, password (if SSO is not used), title, department	Create a customer account Provide Zoom services
Customer content: information you or others upload, provide, or create while using Zoom	Cloud recordings, chat / instant messages, files, whiteboards, and other information shared while using the service, voice mails	Provide Zoom services* Store chat logs (for delivery and so you can review and search chat history) Store recordings, if explicitly requested by the host or Customer Store voice mail for Zoom Phone
Type of Data	**Examples**	**Zoom Uses it to**
Technical information about your devices, network, and internet connection	IP address, MAC address, other device ID (UDID), device type, operating system type and version, client version, type of camera, microphone or speakers, connection type, etc. The phone number of a person making a call using Zoom services (e.g. Zoom Phone)	Connect you to and optimize your experience using our services Provide customers dashboards and reports Respond to requests for support

			Monitor performance of our data centers and networks Conduct anonymized, aggregated analytics to improve Zoom's service performance
	Approximate Location	To the nearest city (we do not "track" your specific location)	Connect you to the nearest data center Comply with privacy and other laws – for example, so we can provide you with the right notices for your area Suggest choices such as language preferences Monitor performance of our data centers and networks Respond to requests for support
	Information about how you use Zoom (this is NOT information or content you share in your meetings or in chats)	Did you use VoIP or a phone call? Did you shift from the mobile client to the desktop?	Optimize your Zoom experience Respond to requests for support Conduct anonymized, aggregated analytics to improve Zoom's performance.
	Setting and preferences chosen by the user	Join with video off Require meeting password	To provide you choices for how you use Zoom

		Enable waiting room Do not allow screen sharing other than host	
	Metadata	Duration of the meeting / Zoom Phone call Email address, name, or other information that a participant enters to identify themselves in the meeting Join and leave time of participants Name of the meeting Date / time that meeting was scheduled Chat status (unless a setting is actively chosen by user) Call data records for Zoom Phone	Provide Zoom services Provide customers dashboards and reports Respond to requests for support
Why the need for a PIA was identified:	Zoom raises a series of issues from a privacy perspective as well as security issues. Information is currently routed through servers in China.		

Step two: Describe the information flows

Collection:	Only with consent and agreement should people sign up to this service. People will need to sign on themselves recognising the risks around data sharing with Zoom.
Use:	Online learning sessions only – no sensitive information should be discussed. People also need to be aware that 'Zoombombing' is a possibility and that appropriate passwords, procedures and security will be required, but may not completely protect against this risk
Deletion	Data will be deleted at the end of use and certainly in the August following a pupil's leaving school, if not before.
Number affected: (anticipated)	272 children (195 @ Laxey; 77 @ Dhoon)
Flow diagram: *(Nb. A simple arrow/flow diagram is helpful, if possible)*	

Consultation requirements (*if applicable)

Practical steps to ensure that risks are identified:	Risks identified: Servers based in China Zoombombing Data shared with Zoom Encryption – not end to end Password protecting meetings
Practical steps to ensure that privacy risks are addressed:	People need to be made aware of what having servers in China means in terms of monitoring. With protective measures in place to reduce risk of 'zoombombing' - meetings should be password protected and the link sent out and not shared. Updated apps / software needs to be used – again this possibility needs to be highlighted to data subjects and their parents. No sensitive information should be discussed using this service. Links and passwords should not be shared widely.
Internal consultation with:	Federation teaching staff.
External consultation with:	Headteachers at Kewaigue, Sulby and RGS (already using Zoom with pupils) Parents via letter – sharing the protocol and requirement for explicit consent. Legal and Admin Manager (DESC DPO) – Andrew Shipley
Consultation methodology *(link to the relevant stages of the project management process):*	Consultation with staff to discuss feasibility. Consultation with parents to seek interest and subsequent permission Consultation with DESC DPO
Dates of consultations:	
Consultation 1: INTERNAL	Staff meeting 19.05.2020 Email exchange with HT at RGS 20.05.2020 Meeting with Sulby HT 21.05.2020 SLT meeting 22.05.2020
Consultation 2: EXTERNAL	Email exchange with DESC DPO 21.05.2020 Letter to parents 25.05.2020

Step three: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

Annex three can be used to help you identify the DPA related compliance risks.

Privacy issue	**Risk to individuals**	**Compliance risk**	**Associated organisation / corporate risk**
Disclosure of personally identifiable information (PII)	Information shared with 3rd parties eg Zoom	Non-compliance with DPA	Non-compliance with DPA or other legislation can lead to sanctions, fines and reputational damage
Data breach esp as encryption – not end to end	PII shared with unknown parties	Non-compliance with DPA	Non-compliance with DPA or other legislation can lead to sanctions, fines and reputational damage
Servers based in China	PII subject to possible review	Non-compliance with DPA	Non-compliance with DPA or other legislation can lead to sanctions, fines and reputational damage
Data being used for purposes other than those it was collected for.	Users have a right to understand how we will use the PII	Non-compliance with DPA	Non-compliance with DPA or other legislation can lead to sanctions, fines and reputational damage

Data being held outside the EU and therefore subject to other jurisdictional legislation	Data protection laws may not be equivalent to IOM, and therefore may not have the same controls	Non-compliance with DPA	Non-compliance with DPA or other legislation can lead to sanctions, fines and reputational damage
Not specifically a privacy issue:			
Zoombombing	Subject to unpleasant materials		Complaints and upset caused. Reputational damage

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (eg the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Information shared with 3rd parties eg Zoom.	Up to date software should be installed. Data subjects to be informed that this is a possibility.	Accepted.	Proportionate – data subjects should not suffer detriment through not using this service if they choose.
PII shared with unknown parties.	No sensitive personal data should be shared. Those signing up to the service should be made aware that personal information will be needed.	The person using the service either accepts this or not – it is their choice.	Proportionate – data subjects should not suffer detriment through not using this service if they choose.
PII subject to possible review.	No sensitive personal data should be shared. Those signing up to the service should be made aware that personal information will be needed – people need to be informed that what they say / do may be monitored as routed through China and also info stored in US.	The person using the service either accepts this or not – it is their choice.	Proportionate – data subjects should not suffer detriment through not using this service if they choose.
Users have a right to understand how we will use the PII.	Limited PII used by school – it is the service being used. Privacy notice to be updated with suitable information and warnings.	The person using the service either accepts this or not – it is their choice.	Proportionate – data subjects should not suffer detriment through not using this service if they choose.
Data protection laws may not be equivalent to IOM, and therefore may not have the same controls.	Privacy shield in place. Privacy notice for Zoom recognises the GDPR principles and privacy and security are areas that they are working on.	The person using the service either accepts this or not – it is their choice.	Proportionate – data subjects should not suffer detriment through not using this service if they choose.

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project?

What solutions need to be implemented?

Risk:	Approved solution:	Approved by (Headteacher / Principal or designate):
Information shared with 3rd parties eg Zoom	Up to date software should be installed. Data subjects to be informed that this is a possibility	Y
PII shared with unknown parties	No sensitive personal data should be shared. Those signing up to the service should be made aware that personal information will be needed.	Y
PII subject to possible review	No sensitive personal data should be shared. Those signing up to the service should be made aware that personal information will be needed – people need to be informed that what they say / do may be monitored as routed through China and also info stored in US.	Y
Users have a right to understand how we will use the PII.	Limited PII used by school / UCM – it is the service being used. Privacy notice to be updated with suitable information and warnings.	Y
Data protection laws may not be equivalent to IOM, and therefore may not have the same controls	Privacy shield in place. Privacy notice for Zoom recognises the GDPR principles and privacy and security are areas that Zoom are working on.	Y

SIGN OFF **DESC DATA PROTECTION OFFICER** **DPIAs should be signed, sent and retained by** **> DPO-desc@gov.im <**

Data Controller signature (Headteacher / Principal):  Date: 22.05.2020

DPO-DESC signature: _____ Date: _____

SIRO signature: _____ Date: _____

Step six: Integrate the PIA outcomes back into the project plan

(Who is responsible for integrating the PIA outcomes back **into the project plan** and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?)

Action to be taken	Date for completion of actions	Responsibility for action
Advise that the most up to date software should be used – patches and updates installed.	25.05.2020 On release.	Users.
When personal data of a sensitive nature starts to be shared the meeting should be terminated and continued more securely, if appropriate – NB safeguarding responsibilities and also protecting staff.	Immediately.	Host (staff member of school)
Privacy notice to be updated to highlight risks and issues	25.05.2020	Executive Headteacher
Consent to be sought before using the service	25.05.2020	

Contact point for future privacy concerns:
Executive Headteacher DPO-DESC

Linking your PIA to the GDPR privacy principles

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

Principle 1
1. Lawfulness, fairness and transparency **Transparency: Tell the subject what data processing will be done.** **Fair: What is processed must match up with how it has been described** **Lawful: Processing must meet the tests described in GDPR** *[article 5, clause 1(a)]*
Have you identified the purpose of the project?
Yes – to provide on-going contact with pupils and students.
How will you tell individuals about the use of their personal data?
Privacy notice; consent form and letter.
Do you need to amend your privacy notices?
Yes – before using the service
Have you established which conditions for processing apply?
Consent is being used – some parents may not want their children / young person using this service.
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?
By email. It is for individual establishments to establish other means of communicating with their students if they are able eg email.
Our organisation (CO) is subject to the Human Rights Act, please also consider:
• Will your actions interfere with the right to privacy under Article 8?
No
• Have you identified the social need and aims of the project?
Yes – to maintain contact with data subjects during this period of lockdown.
• Are your actions a proportionate response to the social need?
Yes; but there are recognised issues with the service so explicit information needs to be provided.
Principle 2
2. Purpose limitations **Personal data can only be obtained for "specified, explicit and legitimate purposes"** *[article 5, clause 1(b)]***. Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.**
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?
No
Principle 3
3. Data minimisation **Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".** *[article 5, clause 1(c)]* *I.e. No more than the minimum amount of data should be kept for specific processing.*
Is the quality of the information good enough for the purposes it is used?
Yes; it is personal choice whether people sign up but it must be made clear what the risks are.
Which personal data could you not use, without compromising the needs of the project?
Limited information is needed by the person controlling the meeting although they are able to access more information than they need due to the set-up of Zoom as it stands.
Principle 4
4. Accuracy **Data must be "accurate and where necessary kept up to date"** *[article 5, clause 1(d)]* **Baselining ensures good protection and protection against identity theft. Data holders should build rectification processes into data management / archiving activities for subject data.**
If you are procuring new software does it allow you to amend data when necessary?
N/A
How are you ensuring that personal data obtained from individuals or other organisations is accurate?
N/A

Principle 5
5. Storage limitations **Regulator expects personal data is "kept in a form which permits identification of data subjects for no longer than necessary".** *[article 5, clause 1(e)]* *I.e. Data no longer required should be removed.*
What retention periods are suitable for the personal data you will be processing?
N/A – up to individuals to delete their accounts as they see fit
Are you procuring software that will allow you to delete information in line with your retention periods?
N/A
Principle 6
6. Integrity and confidentiality **Requires processors to handle data "in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage".** *[article 5, clause 1(f)]*
Do any new systems provide protection against the security risks you have identified?
Security is being developed as part of the ongoing development of Zoom
What training and instructions are necessary to ensure that staff know how to operate a new system securely?
Some input may be needed to ensure meetings are password protected and to show how links are passed out.

Privacy notice amendments / updates:
Covid-19 Zoom for remote sessions

In order to facilitate remote working Laxey / Dhoon School are using a service called Zoom. Please be aware that there are privacy and security issues at present with this and we understand that you may not want to use this service. There is no obligation to do so. Some of the problems have been highlighted in the press and include:

Information routed through servers based in China – possible review of information.

⇒ Sharing of data with Facebook – updated software should be used.
⇒ Zoombombing – suitable passwords should be in place and links should not be shared.
⇒ Encryption is not end to end - No personal information should be shared during sessions as the service is not properly encrypted.
⇒ Non-protected meetings – Only password protected meetings should be held.

The data the Zoom service collects and uses is as detailed below:

Type of Data	**Examples**	**Zoom Uses it to**
Information that identifies you	For customers: Account owner name, billing name and address, payment method Your name, username and email address, or phone number, when you use this information to access or use our services The phone number a Zoom Phone user dials	Create a customer account Provide Zoom services Communicate with a customer Respond to requests for support
Other account data	Your phone number (if you choose to put it in), language preference, password (if SSO is not used), title, department	Create a customer account Provide Zoom services

Customer content: information you or others upload, provide, or create while using Zoom	Cloud recordings, chat / instant messages, files, whiteboards, and other information shared while using the service, voice mails	Provide Zoom services* Store chat logs (for delivery and so you can review and search chat history) Store recordings, if explicitly requested by the host or Customer Store voice mail for Zoom Phone

*Zoom does not monitor or use customer content for any reason other than as part of providing our services. ***Zoom does not sell customer content to anyone or use it for any advertising purposes.***

Data that our system collects from you:

Type of Data	**Examples**	**Zoom Uses it to**
Technical information about your devices, network, and internet connection	IP address, MAC address, other device ID (UDID), device type, operating system type and version, client version, type of camera, microphone or speakers, connection type, etc. The phone number of a person making a call using Zoom services (e.g. Zoom Phone)	Connect you to and optimize your experience using our services Provide customers dashboards and reports Respond to requests for support Monitor performance of our data centers and networks Conduct anonymized, aggregated analytics to improve Zoom's service performance
Approximate Location	To the nearest city (we do not "track" your specific location)	Connect you to the nearest data center Comply with privacy and other laws – for example, so we can provide you with the right notices for your area Suggest choices such as language

		preferences Monitor performance of our data centers and networks Respond to requests for support
Information about how you use Zoom (this is NOT information or content you share in your meetings or in chats)	Did you use VoIP or a phone call? Did you shift from the mobile client to the desktop?	Optimize your Zoom experience Respond to requests for support Conduct anonymized, aggregated analytics to improve Zoom's performance.
Setting and preferences chosen by the user	Join with video off Require meeting password Enable waiting room Do not allow screen sharing other than host	To provide you choices for how you use Zoom
Metadata	Duration of the meeting / Zoom Phone call Email address, name, or other information that a participant enters to identify themselves in the meeting Join and leave time of participants Name of the meeting Date / time that meeting was scheduled Chat status (unless a setting is actively chosen by user) Call data records for Zoom Phone	Provide Zoom services Provide customers dashboards and reports Respond to requests for support

Please be aware that there are privacy and security issues with Zoom. If you have any concerns regarding the use of Zoom please do not download the App or log on to the service.