Corporate Privacy Notice for Nottingham City Council using Zoom for virtual Meetings during Covid 19 Pandemic

Nottingham City Council
Information Compliance

Nottingham City Council
PN-158

May 2020

Zoom is a cloud platform for video, voice, content sharing and chat that can be used across mobile devices, desktops, telephones, and room systems. Zoom will allow meetings to be conducted remotely, so that usual Council duties can be replicated as much as possible during this time period when strict restrictions on interactions and meetings are being observed due to COVID-19. The basis under which the Council uses personal data for this purpose is that this is necessary for the performance of a task carried out in the public interest by the Council or in the exercise of official authority vested in the Council.

(Zoom is just one platform that can be used to facilitate video meetings and interviews. Other platforms such as Microsoft Teams are also used by the council. For more information on Zoom, particularly when children are concerned, please see below an information pamphlet published by National Online Safety).

Zoom may be used in a variety of settings in the Council, including:

- Committee meetings
- Coroner's inquests
- School appeals
- Social care meetings
- Recruitment exercises

All Council meetings that are open to the public and taking place via Zoom will be streamed via YouTube. You will be informed of this in an announcement at the meeting before the Livestream starts.

The personal data that will be collected in order to facilitate meetings and interviews could include:

- Your name (and business address if applicable)
- Your email address
- Your business email address and business telephone number
- Your job title

The personal data that will be required by Zoom in all settings will be:

- Your name
- Your location
- Your IP address
- image/video (if your device camera is switched on)
- voice (if your device microphone is switched on and you participate)

Recordings of meetings will not routinely be retained by Zoom or the Council. When there is a requirement to keep a record, you will be informed. If the meeting is recorded, the following information will be collected:

●image/video (if your device camera is switched on)
●voice (if your device microphone is switched on and you participate

The information provided by you may include the following special categories of personal data, depending on the nature of the meeting, inquest or interview:

- Race and Ethnicity
- Religious or Philosophical views or beliefs Information
- Political views or opinions
- Sexual Orientation
- Trade Union Membership
- Health Data
- Biometric Data, which is used to identify an individual.

Information in these categories is used by the Council on the basis that such use is necessary for reasons of substantial public interest, and in accordance with the provisions of the Data Protection Act 2018.

Please refer to Information Asset Register: https://geoserver.nottinghamcity.gov.uk/information-asset-register/. and the local privacy notice for the area the meeting is in relation to (e.g. Childrens and Adults, or School Appeals) for information on data retention.

The information provided by you may also be used for the purpose of any other function carried out by the Council. Information about these functions and the legal basis on which information is used for them can be found at http://www.nottinghamcity.gov.uk/privacy-statement/.

The Data Controller is Nottingham City Council, Loxley House, Station Street, Nottingham NG2 3NG. The Data Protection Officer is Naomi Matthews. You can contact the data protection officer at the above address or at data.protectionofficer@nottinghamcity.gov.uk .

The new data protection law known as the General Data Protection Regulation provides for the following rights as prescribed by the legislation:

- A right to request a copy of your information
- A right to request rectification of inaccurate personal data
- A right to request erasure of your data known as ‘the right to be forgotten’
- A right to in certain circumstances to request restriction of processing
- A right in certain circumstances to request portability of your data to another provider
- A right to object to processing of data in certain circumstances
- A right regarding automated decision making including profiling

Please note that if you are unhappy with a decision regarding the handling of your data you have the right to complain to the Information Commissioner’s Office at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. See also the Information Commissioners website at https://ico.org.uk/your-data-matters/ .

For more information about these rights please refer to our detailed privacy statement at https://www.nottinghamcity.gov.uk/privacy-statement .

Founded in 2011, Zoom is one the world's leading video conferencing software providers. It has a number of features, including video and audio conferencing, real-time messaging, screen-sharing and the ability to upload, share and search for content. Users can start their own meetings or they can join meetings set up by others. The app is available to use across PCs, laptops, tablets and mobiles phones and is free to download on both the app store and on Android.

What parents need to know about ZOOM

ZOOM BOMBING

'Zoom bombing' is the term which has been coined to describe unauthorised people joining zoom meetings uninvited and broadcasting pornographic or inappropriate videos. An attacker can hijack a meeting if they know the meeting ID and it isn't reinforced with a password. Not taking preventative measures or implementing privacy controls could open up the risk of children witnessing sexual or inappropriate content with very little notice.

RISK OF PHISHING

The rise in popularity of Zoom has led to a rise in hacking operations and phishing campaigns. This is when participants are encouraged to click on links to join what they believe to be legitimate Zoom meetings via email, but which are in fact fraudulent. These scams aim to obtain sensitive information such as user login details, passwords and/or credit card information.

PRIVACY CONCERNS

Depending on how the app has been set-up, Zoom can offer very little privacy. In many cases, the meeting hosts can see detailed information about each participant including their full name, phone numbers and maybe even location data. Furthermore, depending on where the camera has been set up or where your child's computer is positioned, private or personal information could be stolen depending on what can be seen in the background.

LIVE RECORDINGS

One of the features of Zoom is the ability to record live meetings. By default, only the host of the meeting can usually record live sessions however other meeting members can also record if the host gives them access. Recordings can be stored on devices or on the cloud and can be downloaded and shared with no restrictions. This means that videos, audio clips and transcripts of recordings involving your children could be widely shared on the internet or between users without your authorisation or consent.

PRIVATE ZOOM MEETINGS

Zoom has a facility to set up breakout rooms, which enables a private meeting within the main Zoom session. The host can choose to split the participants of the original meeting into separate sessions. This gives children the ability to speak privately away from the main group to other users however chats aren't always monitored by the host and if the meeting has been made public, children could be more vulnerable to experiencing negative comments.

'LIVE STREAMING' RISKS

At its very core, Zoom facilitates live streaming. That means it inevitably carries some of the associated risks that live streaming brings. These are likely to be minimal within a controlled environment (for instance when used in a classroom setting for remote learning). However, live streaming means that content isn't always moderated and children who use the app unsupervised or with limited security settings, may be more at risk of exposure to viewing inappropriate material. Other risks can include downloading malicious links, sharing personal information or even potential grooming.

Safety Tips For Parents

REPORT INAPPROPRIATE CONTENT

Remind your child that if they do see something that makes them feel uncomfortable or upset then they need to talk about it and report it. Parents can report unwanted activity, harassment, and cyberattacks to Zoom directly. To help your child, you could try setting up a checklist before they go online, with an agreed set of rules and what they should do if they see something inappropriate.

USER PRIVATE MEETING IDS & PASSWORDS

It is always better to set up a meeting with a random ID number generated by Zoom than by using a personal number. This means it is harder to guess and less likely to be hacked. It's important to never share meeting IDs with anybody you don't know and always set-up a password function to allow other people to sign-in. This should already be a default setting that is applied on Zoom.

PROTECT YOUR PERSONAL DATA

It's important to discuss with your child that they should not share personal information on Zoom. This includes passwords, their address, phone number, etc. Create your child's account under a false name or pseudonym and always set a custom background to help hide details in your home. Zoom allows you to turn on virtual backgrounds and select your own image to appear behind you.

BEWARE OF PHISHING EMAILS

Every time you or your child gets a Zoom link, it's good practice to ensure it has come from the official platform and is not fraudulent. Signs of a phishing email include an unrecognisable email address, an unofficial domain name or a slightly distorted logo. The email itself might also be poorly written or contain suspicious attachments.

TURN OFF UNNECESSARY FEATURES

If your child is using Zoom, there are a number of features that you can turn off to make the experience safer for them. For instance, disabling the ability to transfer files or engaging in private chats can help to limit the risk of receiving any malicious attachments or receiving any inappropriate messages. In addition, you can turn off the camera if it is not needed or mute the microphone when not in use.

USE THE 'VIRTUAL WAITING ROOM FEATURE

The waiting room feature on Zoom means that anybody who wants to join a meeting or live session cannot automatically join and must 'wait' for the host to screen them before entering. This is now a default function and adds another layer of security to reduce the likelihood of zoom bombing.

KEEP YOUR VERSION UPDATED

It's important to ensure you are using the latest version of Zoom available and always update it if you get a prompt. These updates are usually to fix security holes and without the update you will be more vulnerable to an attack. Check the official website to see what the latest version is and compare it to your own.

HOST IMPLEMENTED PRIVACY CONTROLS

If your child is part of a larger group meeting, then it's important to make sure that the host is abiding by Zoom's Terms of Service. This includes the fact that they have gained everybody's permission for the session to be recorded.
The host should also have set screen sharing to 'host only' and disabled 'file transfer' to help keep the live stream secure.

Meet our expert

Emma Davis is a cyber security expert and former ICT teacher. She delivers cyber awareness training to organisations nationally and has extensive knowledge and experience of managing how children access services and apps online.

National Online Safety®
#WakeUpWednesday

SOURCES: https://zoom.us/privacy | https://zoom.us/ | https://zoom.us/docs/doc/School%20Administrators%20Guide%20to%20Rolling%20Out%20Zoom.pdf
https://www.theguardian.com/technology/2020/apr/02/zoom-technology-security-coronavirus-video-conferencing