CORONAVIRUS

PROTECT YOURSELF & OTHERS

Stay Connected

Nottingham City Council

Nottingham Manager - responding to Coronavirus

Data Protection Advice for using social media to process data with citizens during the Coronavirus pandemic

1. Keep sharing

In an emergency, working with partners and sharing information with them can make a real difference to public safety. In fact, it could be more harmful not to share the data than to share data about vulnerable residents who are housebound due to self-isolation and who need support. We just need to ensure that we do this lawfully and securely.

Data protection law does not prevent you sharing personal information where it is appropriate to do so. The key is to think about what is the minimum amount of personal information you can share and the most secure way to achieve this in the present emergency circumstances.

In an ideal situation we would only use NCC systems, NCC telephones and Microsoft Teams for meetings. However, when there is an emergency such as the latest pandemic you may need to consider alternatives in the short term to stay in touch with vulnerable citizens.

2. Special Data

You should also take particular care if you are handling sensitive data, referred to as ‘special category data’ in data protection law. This is private information like citizen’s health records, sexuality, race, ethnicity and religion. If you are going to use this kind of information, you should ask further questions

- Do I need this information to protect a person at risk (safeguarding individuals)?
- Would this information save someone’s life (vital interests)?

If the answers is ‘yes’ to any of these questions, then you can also handle and share this type of information. Make sure you are doing only what is necessary and appropriate for the task.

3. Meetings

If you can’t manage meetings face to face then you can look for alternatives. There is no reason why you cannot have a telephone conversation with the citizen or you could use alternatives such as:

- **Face Time**

FaceTime is secure and by its nature information cannot be recorded or stored using the app. This can be a viable alternative to face-to-face meetings. However, each party will need an apple i-phone or mac for this to be technically possible.

In the same way that you would record notes of a face-to-face meeting, it is important to take notes of this virtual meeting which should be added to an NCC system such as liquid logic as soon as possible.

- **By telephone to a landline phone/mobile phone**

It is best to use the NCC telephones to conduct a meeting but if that is not possible, you can use your own telephone. However, this should not be used unless it is an emergency as a citizen may then potentially have your personal number. Again it is important to record notes at the time of the telephone meeting and then to add these into your system such as liquid logic.

Please note that text can be used. However, there can still be privacy issues as other members of families may be able to access the text and this is not suitable for sensitive data.

Some mobile phones are connected (for example Apple though family groups) which may mean that messages that you send to one recipients mobile phone can also be seen on multiple gadgets such as I-pods or I-pads, for this reason caution should be exercised in respect of sensitive data.

Telephone calls and meetings must not be recorded by employees for work purposes, unless it is lawful to do so and express authorisation has been given. For further advice please contact the data protection officer at data.protectionofficer@nottinghamcity.gov.uk

Failure to adhere to this may lead to a data breach. Any alleged data breach must be reported to the Information Compliance Team.

- **Microsoft Teams Meetings**

Microsoft Teams is a good way for colleagues to have face to face meetings. You can also share documents via Microsoft Teams with colleagues within the organisation to discuss amendments and to make changes in real time.

Video calls / conferencing via Teams to external parties is also possible. It’s more of a webex style meeting than a call. A webex meeting is an online meeting that allows you to virtually meet with other people. By logging into the meeting via the internet, you will be able to see the presenter’s computer screen. Any NCC staff member can host a meeting in Teams and send a link to any external party for them to join (you can also schedule future meetings and have the links pre-sent). By pressing the three dots icon whilst you are in a video meeting 'blur background' becomes an option. When meeting with a citizen via Teams please ensure that this functionality is used as it will blur out any private information on your screen and protect your privacy.

Teams is the preferred method to video conference with colleagues or service users and should suffice where we are hosting / setting up the meeting (call).

The IT service are currently preparing more detailed guidance on this to explain the features in more detail and this will be available on the intranet shortly.

- **WhatsApp phone/ messaging- (see also full WhatsApp guidance)**

WhatsApp should only be used in emergency situations where it is not possible to reach a citizen by any other means. In such cases, the app should only be used to arrange contact by some other verifiable means, e.g. a meeting or phone call.

All use of WhatsApp must be consistent with the Council's policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

WhatsApp should not be used to communicate with children under the age of 13 in line with the Information Society Service (ISS) provisions (Article 8) of the GDPR.

Messages relating to council business must be retained as part of the organisation's business record. This may involve staff entering details of a message into a Council approved case management or other system.

Messages identified as a council business record will be retained in accordance with the Council's Record Retention Schedule.

Users should not automatically forward messages to a third party. Any individual messages which are forwarded must not contain Council confidential or personal information.

Caution must be exercised with WhatsApp groups as it is easy to forget who else is in the chat group. Group chats should not be used to discuss sensitive personal data unless it is an emergency.

Users should not use WhatsApp to create or record any binding transactions or to store or retain email on behalf of the Council. Such communications and transactions should be conducted through proper channels using Council approved systems.

For further information about the use of WhatsApp please see the full NCC WhatsApp guidance.

- **Skype**

This is another virtual way to conduct a meeting with citizens or partner organisations if they do not have Microsoft Teams

All Skype-to-Skype voice, video, file transfers and instant messages are encrypted. This provides some protection from malicious users.

If you make a call from Skype to mobile and landline phones, the part of your call that takes place over the PSTN (the ordinary phone network) is not encrypted.

- **Zoom**

Zoom should only be used in an emergency where there is no other option and should only be used via a citizen's computer (not via the citizens mobile phone). As set out above Microsoft Teams is the preferred option.

This is due to security and privacy issues with using Zoom.

One concern stems from the fact that when a user downloads the iOS app and opens it on their phone, it communicates with Facebook, sending information such as the model of the user's device, where they are connecting from, what phone network they are on and a special unique code that can be used to identify the device. A separate concern is the default settings of the service, which are configured in the expectation of trust between participants, meaning trolls can cause problems. Trolls have used the screen-sharing feature to broadcast pornography and violent imagery. In addition, security experts have said the file transfer feature that is switched on by default could be used to spread malware. It is therefore important to confirm that only the host can share their screen.

Therefore, if you do need to use zoom for a meeting make sure that you:

- Use laptop and not a phone to access zoom
- Go to Personal Settings and turn off file transfer
- Go to Personal Settings and turn off screen sharing

4. Sharing Documents and sensitive information in emails and email attachments

- **Cryptshare**

For those NCC employees who already have this installed on their computer this is a safe way to send information electronically and the information can be password protected. The citizen can either telephone to get the password or it could be sent through by another means such as text message.

- **Encrypt**

By putting this in the header this will encrypt the e-mail in transit but it will not assist if it accidentally gets sent to the wrong address or someone else accesses the email. As may email accounts are not secure we would also advise you to password protect the document and again they can telephone for the password or it could be sent by another means for example text message.

- **Password Protecting Documents**

When creating a document in word it is possible to create a password for the document so it cannot be processed without the password. This helps to protect the data from unauthorised access.

How to set a password for an Office document

i. Open the **Word** (Excel or PowerPoint) **document**.
ii. Click on **File**.
iii. Click on Info.
iv. On the right side, click the **Protect document** menu. ...
v. Select the Encrypt with **Password** option.
vi. Type a **password** to **protect** the **document**.
vii. Click the OK button.
viii. Retype the **password**.

If citizens need to send information they can also be advised how to password protect their documents or use one of the on-line solutions such as Dropbox. It can be a good way for citizens to send information as it is secure. The subscriber is responsible for the security, which can be made secure, but also made weak.
The citizen can either telephone to get the password or it could be sent through by another means such as text message.

NCC employees should use teams / email / one drive or SharePoint to share documents.

Final Advice

- Be extra vigilant about opening web links and attachments in emails or other messages. Don’t click on unfamiliar web links or attachments claiming to give you important COVID-19 updates. We are seeing a rise in scams so follow the National Cyber Security Centre’s (NCSC) guidance on spotting suspicious emails.
- Use strong passwords. Whether using online storage, a laptop or some other technology it is important to make your passwords hard to guess. See NCC guidance for further information.
- Do you need to send out the information at this time or can it wait until there is a more secure way to achieve this?

For further advice, please contact the Data Protection officer at
data.protectionofficer@nottinghamcity.gov.uk