SAFE WELL PROSPEROUS CONNECTED

Information Governance Framework

Schedule 02D

Digital Technologies Policy

North Lincolnshire Council

www.northlincs.gov.uk

- Add a disclaimer to your blog or social media profile to make it clear that your accounts and views are personal – for example: "The views I express on this platform are my own." – if you have identified the council as your employer.

Inappropriate use of social media, including messaging tools could breach the council's Code of Conduct and may result in disciplinary action.

Council equipment (smartphones and computers, for example) should not be used to access social media in a personal capacity.

14. Recording of Activities

When acting on behalf of the council it is possible that a person or organisation may record the conversation or meeting, or there may be a requirement for a recording to be made. The term 'recording' refers to any means by which a record could be made of interactions, including audio, video and photographs.

Under Data Protection legislation everyone has the right to record their own conversations for their own use or to record public meetings. In these instances there is no requirement to notify the council of the recording or to obtain consent. When someone is acting on behalf of the council it is likely that there should be no reason to refuse any recording.

Recordings by individuals and other parties

Everyone has the right to record their own conversations, however in practice recording telephone conversations or meetings could make those taking part uncomfortable and so may not be helpful to the discussion. Therefore, rather than making a recording, it may be preferable to:

a) Arrange for notes to be taken that could be circulated and agreed afterwards;
b) For questions or issues to be submitted in writing, and a written response provided.

If a meeting is to be recorded both parties should receive a copy of the recording.

If an individual then decides to make a recording available to others (e.g. someone not party to the original call or meeting or someone who is not an intended recipient), consent from the council should be sought first. It might be necessary to provide the council with a copy of the recording for consent to be considered.

Recordings by the council

The council's telephone system is capable of recording conversations. The circumstances when conversations can be recorded are set out in section 3 of the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (LBP Regulations). These circumstances include:

a) To evidence facts;

b) To ascertain compliance with regulatory procedures;
c) To ascertain if standards or targets are being met (and to assist in training);
d) In the interests of national security;
e) For the prevention or detection of crime; or
f) To investigate or detect unauthorised use of a telecommunications system.

To comply with Payment Card Industry Data Security Standards (PCI DSS) and good practice, payment details are not recorded.

If an employee intends to record a non-public meeting or interview the attendees must be informed that recording is taking place and the purpose for the recording.

The council's Privacy Notice includes information about the recording of telephone calls.

Recordings of public meetings

The council supports the principle of transparency and encourages filming, recording and taking photographs at meetings open to the public. We also welcome the use of social media to communicate with people about what is happening at a meeting.

At the beginning of a public meeting, the Chair will make an announcement if the meeting is being recorded by the council or that it may be recorded by a third party. Meeting agendas and / or signage will also notify attendees of this.

Whilst there is no requirement for third parties to notify us in advance, the Chair of the meeting will have absolute discretion to terminate or suspend any of these activities if, in their opinion, continuing to do so would prejudice proceedings at the meeting.

The circumstances in which the Chair can terminate or suspend could include:

a) Disturbance of the meeting;
b) The meeting agreeing to formally exclude the press and public from the meeting due to the confidential nature of the business being discussed;
c) Where it is considered that continued recording / photography/ filming / webcasting might infringe the rights of any individual or otherwise disrupt proceedings; or
d) When the Chairman considers that a defamatory statement has been made.

It is expected that those recording meetings will not edit any media in a way that could lead to misinterpretation or misrepresentation of the proceedings. This includes refraining from editing an image or views expressed in a way that may ridicule, or show a lack of respect towards those being recorded.

The Communications team are able to provide assistance with regard to location and set up, particularly if using large equipment or you have any special requirements, such as additional lighting or flash photography.

Recordings for the purposes of investigations

If the council receives a complaint in relation to noise disturbance (e.g. loud music or barking dogs), we have a statutory duty to take such steps as are reasonably practicable to investigate the complaint.

As part of the investigation, efforts will be made to witness the noise, this can be by diary sheets, reactive or programmed visits, or the use of audio monitoring devices.

Audio monitoring devices will only be deployed when appropriate, by either placing the device:

a) In the affected premises with the consent of the occupier; or
b) Outside the source premises without the knowledge of the occupiers of the source premises.

Complainants and complainees will have been informed about the possible use of an audio monitoring device as part of the investigation process.

Neither of these methods of monitoring require authorisation under the Regulation of Investigatory Powers Act 2000 (RIPA), because:

a) The device placed in the affected premises with the consent of the occupier, is not covert and so would not be directed or intrusive; and

b) The device placed outside of the source premises, is unlikely to be directed as it is unlikely to result in the obtaining of private information about a person, and is unlikely to be intrusive as the recording device is outside of the source premises and is recording the noise as it is heard outside of the source premises.

Any noise captured by the monitoring devices relating to criminal or unlawful activity could be provided to the appropriate agency for further action.

Further Information

- Regulation of Investigatory Powers Act 2000 (RIPA) http://www.legislation.gov.uk/ukpga/2000/23/contents
- Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000 (LBP Regulations) http://www.legislation.gov.uk/uksi/2000/2699/contents/made
- Data Protection Act 2018 https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
- Telecommunications (Data Protection and Privacy) Regulations 1999 http://www.legislation.gov.uk/uksi/1999/2093/schedules/made

- Human Rights Act 1998 http://www.legislation.gov.uk/ukpga/1998/42/contents
- Ofcom are the communications regulator in the UK, and their guidance on the recording of telephone conversations is available here http://www.ofcom.org.uk/static/archive/oftel/consumer/advice/faqs/prvfaq3.htm

15. Access or Removal of Access to Digital Technologies

Managers should contact the ICT Solution Centre to request access to any digital technologies for their employees. They will need to provide details of what is required along with details of the business need.

If access to any digital technology is no longer required the employee's manager should contact the ICT Solution Centre.

16. Glossary of Terms

GDPR – General Data Protection Regulation
M365 – A suite of cloud based Microsoft products (MS Teams, Word, Excel, Outlook, etc)
DPA 2018 - Data Protection Act 2018
ICT – Information and Communication Technology
PIN – Personal Identification Number
Jailbraking / Rooting – Removing all restrictions on a mobile device
SIM Card – A microchip in a mobile device that connects it to a particular phone network
MDM – Mobile Device Management
Antivirus – Software that is created specifically to help detect, prevent and remove malware (malicious software) and viruses from computers and devices.
App – Applications
BYOD – Bring your own device
PSN - Public Services Network
CoCo - Code of Connection
FOI – Freedom of Information
EIR – Environmental Information Regulations
SAR – Data Protection Subject Access Request
MoveIT – System for sending encrypted emails to third parties, when general council email is not secure.
Two-factor authentication – Where two forms of identification are needed for access.