Report of the Director
of Governance and Partnerships

Decision to be taken after:
18 February 2021

NORTH LINCOLNSHIRE COUNCIL

FINANCE AND GOVERNANCE
CABINET MEMBER

DIGITAL TECHNOLOGIES POLICY UPDATE

1. OBJECT AND KEY POINTS IN THIS REPORT

1.1 To consider and approve an updated Digital Technologies Policy

1.2 The key points in this report are as follows:

- ➢ The Digital Technologies Policy sets out the way in which information should be securely handled and managed across various IT and digital platforms.
- ➢ The policy has been comprehensively updated and is proposed as a new inclusion to the Information Governance Framework.

2. BACKGROUND INFORMATION

2.1 Information is a key council asset and it is crucial that it is looked after with the same care as other important assets, such as finance, people, land and property.

2.2 The Information Governance Framework comprises a series of specific policy and procedural schedules relating to the management and security of information and personal data. They set out how the council will comply with legal and best practice requirements governing information management. These requirements include the UK General Data Protection Regulation / Data Protection Act 2018 and the Freedom of Information Act.

2.3 The Digital Technologies Policy previously formed part of a suite of policies contained within the HR framework given its original focus on staff conduct issues. However over time the emphasis of the policy has changed to, primarily, the management and protection of information associated with IT use and as such is now considered to be more appropriately aligned with the Information Governance Framework.

2.4 The policy (appendix 1) has been updated to ensure that it continues to reflect the latest digital operating environment. Key changes include:

- New provisions regarding the use of alternative virtual meeting platforms (Section 6)
- Updated guidance on the use of Messaging Tools for business use (section 7)
- The expansion of the Bring Your Own Device section to include new enabling provisions supporting an “agile organisation” (Section 8)
- New inclusions regarding printing when remote working (section 9)

- Development of the social media section (Section 13)
- Enhanced provisions regarding the recording of meetings and conversations and implications for their disclosure under information regulations (Section 14)

2.5 The policy is proposed for further review in Quarter 2 2021 to reflect the implementation of the Microsoft M365 suite of products, associated learning and protocols for their use moving forward.

3. OPTIONS FOR CONSIDERATION

3.1 Option 1: Approve the updated Digital Technologies Policy as a schedule to the Information Governance Framework.

3.2 Option 2: Amend or reject the updated Digital Technologies Policy as a schedule to the Information Governance Framework.

4. ANALYSIS OF OPTIONS

4.1 Option 1 is recommended to ensure that the policy reflects current digital technologies in use and updated legislation and national guidance.

5. FINANCIAL AND OTHER RESOURCE IMPLICATIONS (e.g. LEGAL, HR, PROPERTY, IT COMMUNICATIONS etc.)

5.1 The Information Governance team will lead and support the implementation of the revised policy and its embedding across the council.

5.2 Failure to comply with Information Governance legislation can result in the Information Commissioner imposing significant fines under the UK General Data Protection Regulation / Data Protection Act 2018.

6. OTHER RELEVANT IMPLICATIONS (e.g. CRIME AND DISORDER, EQUALITIES, COUNCIL PLAN, ENVIRONMENTAL, RISK etc.)

6.1 Not applicable.

7. OUTCOMES OF INTEGRATED IMPACT ASSESSMENT (IF APPLICABLE)

7.1 Data Protection is an integral part of the Integrated Impact Assessment and no adverse impacts have been identified. The Digital Technologies Policy makes provision to meet the equality and privacy needs of individuals.

8. OUTCOMES OF CONSULTATION AND CONFLICTS OF INTERESTS DECLARED

8.1 Consultation has taken place with the Joint Consultative Committee (JCC) with no adverse comments or concerns received.

8.2 No conflicts of interest have been identified.

9. RECOMMENDATIONS

9.1 That the updated Digital Technologies Policy (Appendix 1) is approved.

9.2 That the policy is formalised as a new schedule to the Information Governance Framework.

DIRECTOR OF GOVERNANCE AND PARTNERSHIPS

Church Square House
30-40 High Street
SCUNTHORPE
North Lincolnshire
DN15 6NL
Author: Phillipa Thornley/Martin Oglesby/Jason Whaler
Date: 9 February 2021

Background Papers used in the preparation of this report

ICO Guidance
Relevant legislation and guidance

Appendix 1 – Digital Technologies Policy

SAFE WELL PROSPEROUS CONNECTED

Information Governance Framework

Schedule 02D

Digital Technologies Policy

North Lincolnshire Council

www.northlincs.gov.uk

Background Information	
Document Purpose and Subject	To provide a council-wide policy for the use of Digital Technologies as part of the Information Governance Framework.
Author	Information Governance Team.
Document Owner	Information Governance Team.
Change History	V1.2 – Previously part of the NLC HR Manual
File Location	Information Governance Team Shared File Location
Retention Period	Permanent Preservation as a Core Policy
Issue Date	………………..
Last Review	Previously part of the HR Manual
Current Review	February 2021
Next Review Date	May 2021
Approved By	Cabinet Member
Approval Date	………………..

Contents

1. Introduction

Information is an important and valuable business asset which needs to be suitably protected from a wide range of risks and threats including:

- malicious software
- unauthorised access
- computer misuse
- information technology failures
- human error
- physical security threats

This ensures that information is handled appropriately and business continues as usual minimising business damage and maintaining the council's reputation.

The rapid rise of digital technologies has allowed council employees to work in different but more effective agile ways to deliver efficient services to individuals.

To ensure that the council's information remains properly managed and secure we must consider which digital technologies to make use of and ensure that they are used in a controlled way.

This policy sets out how digital technologies should be used within North Lincolnshire Council.

2. Scope

This policy applies to all council employees and all individuals or organisations acting on behalf of the council.

Schools, who are Data Controllers in their own right, may choose to adopt this policy. Where this is not the case, it is expected that they will have their own appropriate policy.

3. General Guidance and Security Incidents

Employee usage of digital technologies will be reasonably monitored where necessary. Employees waive any right to privacy in anything they create, store, send or receive when using the council's digital technologies.

Digital information is stored in line with the General Data Protection Regulation (GDPR) / Data Protection Act 2018 (DPA). As such, digital information may need to be provided in response to Subject Access Requests. Requests for information may also be made under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004.

This policy should be read in conjunction with the council's Information Security Policy, ICT Security Policy and the council's Code of Conduct. Employees should note that breaches of these polices and code may result in disciplinary action.

When using the council's digital technologies, employees must:

- adhere to this policy. This includes where council equipment and personal devices are used.
- keep PIN code or passwords secure and not divulge them to any other person.
- contact the ICT Solution Centre in the event of a forgotten password or use the automated password reset tool.
- inform the Data Protection Officer if you believe there has been an actual or potential data breach – informationgovernanceteam@northlincs.gov.uk or 01724 296302.
- inform the ICT Solution Centre without undue delay if your council or personal device has been compromised, lost or stolen so that any council data can be remotely and securely wiped or the access to it removed, and any mobile telephone numbers blocked.
- if a mobile device, including basic mobiles, smartphones or tablets become compromised, lost or stolen, this must be reported to the ICT Solution Centre as soon as possible, ideally within 24 hours. ICT can apply stolen bars to SIM cards and mobile phones numbers to prevent unauthorised use. Devices may also be able to be traced to a last known location to assist with quick recovery.
- during out-of-hours such as weekends, employees are required to contact the network provider to report a lost or stolen handset so that call barring can be applied. Employees are then required to report the incident to the ICT Solution Centre on the next available working day.
- employees using personal devices must also report the loss or theft to the ICT Solution Centre. This is to allow and execute a remote wipe command which will delete the MDM application and council data from the device or remove access to the data.
- inform your manager if you suspect a colleague has misused digital technologies.
- consult the user guides in the ICT Services knowledge base on TOPdesk for support in the first instance, prior to contacting the ICT Solution Centre.

4. Council Mobile Device Guidance

Where there is a valid business case the council provides employees with a mobile device for use in connection with their work. Personal mobile devices must not be used in connection with council business other than in accordance with section 7.0 of this policy.

Mobile device requests are submitted via the online e-form. To minimise expenditure on mobile devices, ICT Services must be satisfied that at least one of the following business criteria is met, before authorising the issue of a mobile device:

- The employee is a remote worker and requires a mobile device to enable them to undertake their job effectively.
- Issuing the employee with a mobile device will enable them to provide a more efficient service to their customers.
- There is a requirement for the employee to be contactable whilst working away from their normal place of work and where other methods of communication, for example email, are unsatisfactory.
- The employee’s role involves out-of-hours support, for example they are on call, which necessitates an alternative means of contact.
- The employee is a lone worker and their personal safety could be compromised if they are not in possession of a mobile device. However, a mobile device should not be relied upon as the sole means of ensuring an employee’s personal safety. A health and safety risk assessment should be carried out to assess this requirement.
- The employee travels and visits areas where summoning help, if they break down, for example, may be difficult.
- There is a statutory or corporate requirement for a mobile device, for example emergency planning.

Pool mobile devices are available upon request from ICT Services for temporary arrangements and to avoid the need for the council to take out additional contracts.

All council issued mobile devices with internet access, for example smart phones and tablets, are centrally managed. This includes the ability to remotely wipe lost or stolen devices or remove access to data and update anti-virus software where required.

When using a council mobile device employees must **not:**

- call directory enquiries. Phones which have access to the internet should be used to obtain numbers or where necessary a colleague with internet access in the office should be contacted.
- call any number other than UK landlines or UK mobile numbers.
- remove any software that has been installed by ICT Services, for example remote management MDM software or anti-virus.
- disable security configurations which have been applied to the device.
- tamper with or remove the manufacturer’s software restrictions (i.e jailbreaking or rooting the device).
- install any software applications including the use of vendor ‘app’ stores, for example Google Play Store or Apple Store). ICT Services can install

authorised third party apps onto devices. These will be deployed via the MDM system.

Employees are responsible for ensuring the safekeeping of their device at all times and that a PIN code or password is applied when the device is not in use. Employees must ensure that they are not overlooked when entering the PIN or password.

Employees must change the PIN or password on the device to something other than the default PIN or password, using the following guidelines. PIN codes and passwords must:

- be at least five characters in length (four characters where this has been configured by ICT Services).
- contain a mixture of letters and numbers and a combination of uppercase, lowercase, numbers and special characters is recommended.
- be as random as possible, and not contain recognisable words or any other strings associated with the user.

PIN codes and passwords must not:

- use consecutive or the same digits, such as 0000, 123456 or 11111.
- contain more than two identical characters.

Employees must not save personal and sensitive information onto the device, such as the contact details of clients or door codes to council premises.

Employees must not use a hand held mobile device whilst driving. It is an offence to use a mobile device, which is not fitted with a manufacturer installed, loud speaker hands free system. Any other hands-free equipment, including those that require the use of a headset are not acceptable. You should be aware that use of a mobile device whilst driving, even with manufacturer installed loud speaker hands free systems, should be avoided due to the effect on concentration whilst driving.

Mobile devices provided by the council remain the property of the council. When an employee leaves the council it is the responsibility of the employee’s manager and the employee to ensure that the mobile device is returned at the point of leaving, or earlier if requested to do so.

In the event that the employee fails to return the mobile device, the employee’s manager must inform the ICT Solution Centre as soon as possible.

If an employee fails to return the mobile device to the council they will be held responsible for any usage and line rental incurred until the mobile device is either returned to the council or disconnected. An invoice will be issued and sent to the employee to recover the full replacement cost of the equivalent handset, call charges and rental costs plus VAT.

The council may withdraw mobile devices at any time if, for example, it is found that the criteria for issue are no longer met or there has been recognised misuse of the phone.

Lost, compromised or stolen devices must be reported to the ICT Solution Centre as soon as possible so that mobile numbers can be blocked and devices remotely wiped or access to data removed to prevent unauthorised use.

5. Microsoft 365 (M365) Products

M365 is a line of subscription services and tools offered by Microsoft as part of the Microsoft Office product line. These include, MS Teams, Outlook, Word, Excel, OneDrive, and form part of the standard “IT desktop” for employees.

Data consumed in the M365 environment is stored and managed by Microsoft in the “cloud” and is subject to the security protocols associated with this environment.

The council’s use of M365 is relatively new and a series of guidance documents have been produced and made available for employees to follow via TopDesk. The policy section associated with M365 will be updated later in 2021 as knowledge of the product set matures.

6. Video Calling Software

Our default system for hosting video calls is Microsoft Teams (M365) which will ultimately replace legacy use of the former default system, Skype for Business. Microsoft Teams can be used to video call external individuals where they have a Microsoft account.

There are many other platforms and tools that other organisations and individuals could and do use to make video calls, such as Zoom, FaceTime and Facebook Messenger.

Employees can join calls using these other platforms via a browser but are not permitted to host a call using these platforms due to the likelihood of introducing security risks onto the council network, the possibility of hacking and additional license requirements

7. Social Media Messaging Tool Guidance

Our default system for instant messaging internally is Microsoft Teams (M365) which will ultimately replace legacy use of the former default messaging system, Skype for Business. Microsoft Teams can be used to instant message external individuals where they have a Microsoft account.

There are other social media messaging tools that can be installed on smartphones. Due to privacy, security and third-party misuse risks these tools must only be used for official business purposes in exceptional situations when the council's default messaging solution is not available or is unsuitable. Permission to use a social media messaging tool for official business purposes other than the council's default platform is subject to the approval of the Data Protection Officer and IT Security Practitioner.

It should be noted that the use of alternative messaging platforms is kept under constant review by the Data Protection Officer and any permitted use for official council business could be withdrawn at short notice.

Employees should be aware that where social media messaging tools are used for official business purposes and create records of the council's business, these must be stored and retained as explained in the Records Management Policy. In addition, social media messages from any tool used for official business purposes are potentially releasable in response to requests for information such as Freedom of Information.

Employees are reminded of the social media guidance in section 13 below and that inappropriate use of social media platforms, including instant messaging functions, could breach the council's Code of Conduct and may result in disciplinary action.

Where other social media messaging tools are approved for official business use:

Employees **must:**

- assume that any content is in the public domain.
- request the app via the ICT Solution Centre so that ICT Services make the app available to you.
- read the App's 'terms of service, terms and conditions, privacy and acceptable use policies'. These explain how to use settings in your account should you wish to opt out of cookie settings, advertisements, sharing data with third parties and location. Data about you may be collected and used for various purposes some of which can be controlled.
- keep your mobile device and the social media messaging App up to date with the latest software versions.
- keep anti-virus software up to date.
- set up two-factor authentication on your device and choose strong passwords that are different to your corporate or personal accounts
- be aware of scams, hoax/fake news, suspicious messages and warnings that try to get you to click on links or request your personal information.

You must **not**:

- **use other social media messaging Apps to communicate any content that should not be in the public domain, such as personal, sensitive or commercially sensitive information**.

- use any other social media messaging App for transferring corporate documents – please use your council email or secure MoveIT email for those purposes.
- share your passwords, verification or security codes with anyone

8. Bring Your Own Device (BYOD) use of Personal Devices

Employee owned smart phone and tablet devices may be used to access council applications such as email, calendar, contacts and tasks, or other authorised apps such as M365 products. This is only possible where the employee device is configured with the council Mobile Device Management (MDM) software.

It is expected that by taking advantage of the BYOD facilities that employees will hand back their council devices to contribute towards reduction of devices and demand management initiatives.

Before MDM software is installed employees will be asked to:

- Review Microsoft privacy information to understand what information Microsoft can see
- A application protection policy is in place to protect and manage access to council applications from personal devices
- Download and install an authentication tool

The MDM software checks to see if the device meets the council's compliance and ICT security policies.

Employees will be able to use their personal device in the same way as they would any council device and must fully comply with this policy. Non-compliance could mean access to council data on the personal device is removed and the employee may face disciplinary action.

On an employee personal device, the council **can't;**

- View browsing history
- See personal emails, documents, contacts, or calendar
- Access passwords on personal devices
- View, edit or delete photos
- See the location of your personal devices
- See your biometric login information, such as your finger print or facial recognition data.

On an employee personal device, the council **can;**

- View the model, serial number, and operating system of the device

- Identify the device by name
- Prevent access to the applications on the device
- View information collected by council related apps, such as when the app was last accessed.

To manage the personal device the council can, without the permission of the employee, carry out the following functions:

- Disable the council workspace by preventing access to the apps on the device.
- Apply a pin code to each council app. Employees must ensure that they are not overlooked when entering the PIN and that they use a different PIN to that used previously.
- Review and interrogate the communications log. This will only be carried out for trouble shooting, support purposes or for event or incident investigations.

Employees must comply with the following user responsibilities:

- Keep the device up-to-date with anti-virus software and o/s updates
- Back up their device regularly
- Repair and maintain the personal device.
- Be aware that any business use may increase data plan usage and that employees are responsible for any overages and monitoring of usage.
- Employees are responsible for ensuring the safekeeping of their device.
- A password or pin code is set that is applied when the device is not in use and also to access council apps.
- Employees must ensure that they are not overlooked when entering the PIN or password.
- Use a different password to that used for other applications or systems.
- Ensure the device is kept secure at to prevent loss, compromise or theft.
- Not allow others to view or access any council information on your device (shoulder surfing, disclosing to family and friends).
- Not attempt to tamper with or remove any of the security settings that have been applied to safeguard the data on the device.

Employees must not:

- Remove or modify manufacturers settings within the device operating system (i.e. jailbreak or root devices).
- share the PIN code to access the council email system.
- attempt to copy council data onto and off the personal device. The application protection policy will prevent this.

The following security controls will be applied to ensure information is kept secure and to prevent unauthorised access if the device is lost, compromised or stolen:

- After 10 attempts the application protection policy will ask the user to sign in to the application using their council email address and usual login password.

The user will also be asked to approve the sign in via the authenticator or by an authentication phone call.

- The application will lock after 1 minute of inactivity requiring re-entry of the employee's application PIN number.
- Employee access to council applications on personal devices will be remotely removed when the employee leaves the council, if the device is lost or stolen or the employee fails to adhere to this policy.
- Council data is encrypted in the cloud.
- Use of an encrypted channel when council data is in transit over the internet to and from the cloud.
- Employees should be aware that council emails sent from any device must be encrypted where necessary e.g. personal/sensitive information is included and must only be sent using the employee general email account.
- Restriction of the council from accessing other features on the personal device, such as personal internal storage media, camera, Bluetooth and employee personal email accounts.
- Restricting the content of alerts that appear on the device front screen to protect personal and confidential council information.

.

The council does not provide any support for employees' devices, only the council's MDM solution installed on them. The use of an employee's device for business use, accessing the council's system and the installation of the MDM workspace is solely at the employee's risk and discretion. The council does not accept any liability for any loss or damage resulting from the use of the device in any capacity nor as a consequence of the installation or use of the corporate workspace. Employees should be aware that the council will not reimburse the employee for any call charges or data usage charges incurred through using their personal devices for council business.

The council will not refund any business calls made on a personal device unless they are authorised by the relevant Director.

Employees must contact the ICT Solution Centre when you no longer require the MDM 'app' for example, upon leaving the authority or if they intend to sell, recycle, give away or otherwise dispose of the device.

If the employee's personal device is lost or stolen or if they leave the council they must report this to the ICT Solution Centre as soon as possible. In such cases, or if the employee leaves the organisation, the council will remotely remove access to the application.

The UK law on Data Protection only permits export of personal data to certain countries. Where there is a satisfactory adequacy decision in place BYOD can be used outside of the UK. Employees wishing to use their BYOD outside of the UK where there is no adequacy decision must first seek the approval of their Service Manager or above. In these instances the Manager should contact the Data

Protection Officer so that a risk assessment can be carried out before BYOD is taken there.

9. Printing

Printing should always be by exception in circumstances where a digital format is unsuitable or unavailable. Employees have the option of printing documents via the Facilities Management Team using the TopDesk request form and also have access to multi-functional devices located within council managed sites. In addition where more extensive printing is required, approved third-party organisations are contracted to provide a secure printing service.

You must only use a personal printer for the printing of personal, sensitive or commercially sensitive information in exceptional circumstances and only where your line manager has approved this. The storage and disposal of printed material should follow the procedures and rules set out in the Information Security Policy. These provisions apply to printing from council issued devices where the home printing facility must be enabled by ICT Services and also printing from personal devices. Importantly you must not send council emails to your personal email address for home printing purposes. Care should be exercised where printing is enabled with devices that have “wireless” or “air” printing capabilities such as iPads. Use of these devices for printing is subject to the provisions set out above.

10. Email Guidance

The council operates a corporate email facility that provides employees with an email address for use in connection with their work. These guidelines also apply to all users accessing email on council provided mobile devices – smartphones, tablets and BYOD (covered in section 7).

When using the council’s email system, you should **not:**

- use a council email address for personal purposes. The personal use of an email address for employee benefits, medical or schooling/child care purposes is permitted.
- send or forward emails containing offensive or disruptive content, which includes, but is not limited to defamatory, offensive, racist or obscene remarks. If you receive an email of this nature, you must promptly notify the ICT Solution Centre to record this.
- send ‘junk’ emails, chain mail, photos, jokes and executable files of a non-business nature. All messages distributed via the email system are the property of the council.
- send unsolicited email messages.
- forge or attempt to forge email messages.
- disguise or attempt to disguise identity when sending email.
- send email messages using another person’s email account.

- send unnecessary attachments, use document links as an alternative when possible. The ICT Solution Centre will provide assistance if required.
- distribute information regarding items for sale, public events, and general site specific council news. The email system may be used to inform colleagues of specific employee news items, for example colleagues leaving or giving birth.
- reply to emails requesting information such as, bank account details, PIN numbers, passwords or personal information.

When using the council's email system, you should:

- ensure other council email users can view your calendar at all times and where work patterns allow, set your standard working hours within your calendar.
- set your 'out of office' message for both internal and external emails when absent from work.
- delete any suspicious emails in your inbox and report them immediately to the ICT Solution Centre.
- ensure that calendar entries do not disclose information relating to third parties and are marked as private as appropriate.

All generic email accounts must be accessed via an employee's individual email account as part of the Public Services Network (PSN) Code of Connection (CoCo) compliance. If you are emailing confidential information outside the council you must encrypt your messages to make them and any attachments secure.

MoveIT or other permitted platform should be used to send confidential information to other councils and government departments.

When an email has been sent in error and a request to delete the email is made, the request must come from your manager via the ICT Solution Centre. Deleted emails can only usually be restored if, an investigation takes place, on the recommendation of the Data Protection Officer when FOI, EIR or Subject Access requests are made or at the discretion of ICT Services.

Personal email accounts like Gmail or Yahoo, must not be used for council business.

When an email user leaves the council, their entry in our address book will be deleted, the mail file for that person will be saved for a period of 30 days. Access to the user's mailbox or the forwarding of the user's mail can only be gained through manager authorisation.

11. Internet Guidance

The council provides internet access to employees for use in connection with their work. You may use the council's Internet provision for personal reasons but you should not use it:

- during working hours, unless during breaks.
- when members of the public are (or could be) present.
- to run a private business.
- to access any of the following types of website: Adult material, dating, hacking, download sites (including software, or audio/video), illegal websites, storage, peer to peer sharing, online gaming or malicious websites (for example spyware, phishing or fraud sites).

If a website is currently blocked under one of the above categories and access is required for business use, it is possible for access to be granted. A request should be logged with the ICT Solution Centre, which sets out the business need.

The council is not responsible for any personal transactions you enter into (for example, in respect of the quality, delivery or loss of items ordered). You must accept responsibility for, and keep the council protected against, any claims, damages or losses which might arise from your transaction (for example, in relation to payments for the items or any personal injury or damage to property they might cause).

The council is committed to keeping children safe and as part of this commitment it promotes the ethos that safeguarding children is everybody's business. The internet is another tool by which a child could be harmed. The council is committed to ensuring that within the organisation the internet is used to enhance working practice and not to be misused in a way that can harm children and young people.

The use of personal mobile devices logged onto the council's guest wireless network are also subject to this policy, for example smart phones and tablet devices.

12. Wireless Networks and Wi-Fi Hotspots

Public wireless networks or wifi hotspots make it easier to use the internet in places, such as hotels, cafés and conference centres, but accessing the internet in this way introduces the security risk of the information you are accessing online being intercepted, such as by capturing passwords or private emails or by someone creating a spoof hotspot that fools you into thinking it is the legitimate one.

To use public wifi hotspots safely you must:

- use trusted or well-known commercial hotspot providers such as BT Open Zone.

- check with the location vendor the actual hotspot name and look for the padlock symbol to ensure you select the correct secured and encrypted wifi hotspot.
- use a secure web page when browsing the internet (https).
- ‘forget’ the free wifi network in your wifi settings when you have finished.

To use public wifi hotspots safely you must not:

- use suspicious free wifi networks.

13. Social Media Guidance

Professional use

The Marketing and Communications team manage the council’s main social media platforms (Facebook, Twitter and Instagram). They also require access to any other social media accounts and pages within the council.

The Social Media Officer sits within the Marketing and Communications team, and it is their responsibility to survey all council managed social media platforms to ensure they are being used frequently, effectively and professionally.

Social media accounts can be requested by service areas and teams from the Social Media Officer to allow them to; promote their services, engage with the public or businesses, or to generate discussion.

Managers can make the request for a social media account through the social media request form on TOPdesk. The Social Media Officer will consider the requests and grant access to the relevant platforms should they deem their creation necessary.

If a social media account or page is created without the appropriate permission, they must be deleted and re-applied for through the correct channels.

Please note that all council managed social media platforms are reviewed every six to 12 months. If they are found to be unused, ineffective, unprofessional or no longer necessary then they will be removed.

All staff members that administrate a social media account need to be trained by the Social Media Officer. Only once they complete the training can they have full administrative rights to a council managed social media account.

Single log in council managed social media accounts – like Twitter and Instagram – must have strong passwords, which are changed regularly in accordance with the council’s Information Security Policy.

Employees are reminded that while using council managed social media accounts, they are representing the council at all times. Any reputational damage done by a page will be held accountable to the administrator of that page.

Administrators of social media accounts should familiarise themselves with copyright laws and General Data Protection Regulation (GDPR), to avoid any incidents.

Live streaming functions within social media platforms present a significant risk and are strictly forbidden.

Employees breaching the council's Code of Conduct may face disciplinary action.

Personal use

Any employee using social media in a personal capacity is reminded that they are personally responsible for anything they say online, and that what they say can be accessed around the world within seconds; it may be shared or re-published elsewhere and will continue to be available indefinitely.

They should also be mindful that even if information they share, including through instant messaging tools (such as WhatsApp) is restricted to their 'followers', it is in effect public as you cannot control what they do with any information you post – they might screenshot it, for example.

Employees that make personal use of social media outside of work are advised that whilst views and opinions they express are their own, as an employee you are still a representative of the council and you should be aware that any information you post about the council cannot be entirely separate from your working life.

Anyone that makes personal use of social media outside of work should not identify their employer or role in order to avoid any confusion as to whether they are speaking as an employee or individual.

Employees should follow these guiding principles when using social media in a personal capacity:

- Respect the privacy of others and make sure you don't publish any information that is confidential.
- Stay within the law and be aware that defamation, copyright and privacy laws, amongst others, apply.
- Be aware that participating online in a personal capacity may attract media interest in you as an individual, so proceed with care.
- Make sure you avoid any misunderstanding about whether you are speaking as a representative of the council or in a personal capacity.

- 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.