Report of the Assistant Director
Human Resources

Decision to be taken after
19 September 2014

NORTH LINCOLNSHIRE COUNCIL

POLICY AND RESOURCES CABINET MEMBER

DIGITAL TECHNOLOGIES POLICY

1. OBJECT AND KEY POINTS IN THIS REPORT

1.1 To outline and seek approval for the council's revised Digital Technologies policy.

2. BACKGROUND INFORMATION

2.1 The council's Digital Technologies policy is essential in governing how employees use internet, email, social media and mobile devices. Any misuse of digital technologies could cost the council money and potentially damage its reputation. The purpose of this policy is to make clear the standards expected when using digital technologies.

2.2 Each year the council are subject to the Public Sector Network (PSN) Code of Connection controls. In the 2013/2014 submission we were instructed to provide a more secure way of accessing council data via unmanaged end point devices i.e. outside of the council infrastructure via PCs, laptops, tablets and smart phones.

2.3 NLC web mail access was removed in 2014 and a new secure way of accessing email was introduced to employees and schools, which includes a two factor authentication solution.

2.4 Blackberry Enterprise Server Version 10 (BES10) was also purchased to provide a more secure solution and enable the management and control of mobile devices such as tablets and smart phones. This includes all operating systems; Apple iOS, Blackberry, Android and Windows. BES10 was also purchased to assist with mobilising the workforce i.e. to push council data securely to NLC corporate mobile devices. This new solution will also enable access for employees using their personal devices.

2.5 The policy has been updated to reflect these new management arrangements for mobile devices used across the council. This extends to

employees who choose to use their personal devices to access the new corporate workspace. The revised policy provides robust guidance on the remote management of mobile devices, both corporate and personal.

3. OPTIONS FOR CONSIDERATION

3.1 To approve the revised policy.

3.2 To reject the revised policy.

3.3 To recommend amendments to the revised policy.

4. ANALYSIS OF OPTIONS

4.1 Accepting the revised policy will ensure that employees are clear on how mobile devices are managed by the council.

4.2 Rejecting the revised policy would result in a lack of clarity around the management of mobile devices.

4.3 Recommending further changes to the revised policy would require further consultation and delay implementation.

5. RESOURCE IMPLICATIONS (FINANCIAL, STAFFING, PROPERTY, IT)

5.1 There are no resource implications.

6. OUTCOMES OF INTEGRATED IMPACT ASSESSMENT (IF APPLICABLE)

6.1 An integrated impact assessment (see attached) has considered the equality implications of this policy.

7. OUTCOMES OF CONSULTATION AND CONFLICTS OF INTERESTS DECLARED

7.1 The trade unions have been consulted and are in agreement with the proposals.

8. RECOMMENDATIONS

8.1 That the revised policy be approved.

DIRECTOR OF POLICY AND RESOURCES

Civic Centre
Ashby Road
SCUNTHORPE
North Lincolnshire
DN16 1AB
Author: Rebecca Stanford/Richard Bulmer
Date: 20 August 2014

Background Papers used in the preparation of this report: None

1.0 Introduction

1.1 This policy provides the necessary governance rules and principles that apply to employees when using digital technologies, including:

- Email
- Internet and Intralinc
- Social media
- Mobile devices including mobile phones, smart phones and tablets.

1.2 This policy will be reviewed regularly to ensure that it remains relevant and also that any new digital technologies are included as appropriate.

2.0 General guidance

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

2.2 This policy should be read in conjunction with the council's Code of Conduct and any breaches of this policy may lead to action being taken in accordance with the council's Disciplinary procedure.

2.3 When using the council's digital technologies, you:

- Should not give your password to any other person.
- Should telephone the IT Solution Centre in the event of a forgotten password or use the automated password reset tool.
- Should inform the IT Solution Centre if you believe there has been a breach of the IT Security policy.
- Should inform your manager if you suspect a colleague has misused digital technologies.

3.0 Email guidance

3.1 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 (e.g. Blackberry/iPad users).

3.2 Some personal mobile devices with Internet access (e.g. Windows, Apple, Blackberry 10 and Android smart phones and tablets) may be used to access work email. This is covered at section 7.0.

3.3 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 IT 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 IT 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 e.g. colleagues leaving or giving birth.
- Reply to emails requesting information such as, bank account details, PIN numbers, passwords or personal information.

3.4 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 when absent from work.
- Leave any suspicious emails in your inbox and report them immediately to the IT Solution Centre.

3.5 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.

- The PSN email should be used to send confidential information to other councils and government departments.

- For all other confidential emails, our own internal encryption should be used. Please contact the IT Solution Centre for these facilities to be set up on your account.

3.6 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 IT Solution Centre. Deleted emails can only usually be restored if, an investigation takes place, FOI requests are made or at the discretion of IT Services.

- Personal email accounts (e.g. Google mail, Yahoo mail etc.) must not be used for council business.

- When an email user leaves the council, their entry in the North Lincolnshire 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.

4.0 Internet and Intralinc guidance

4.1 The council provides Internet and Intralinc access to employees for use in connection with their work.

4.2 You may use the council's Internet provision and Intralinc 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 (inc. software, MP3 or other audio/video); illegal websites; personal networking and storage; peer to peer sharing; online gaming or malicious websites (e.g. spyware, phishing or fraud sites.)

4.3 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 to a user or groups

of users. A request should be logged with the IT Solution Centre, which sets out the business need.

4.4 The council is not responsible for any personal transactions you enter into (e.g. 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 (e.g. in relation to payments for the items or any personal injury or damage to property they might cause).

4.5 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.

4.6 The council operates Managing Allegations against People who work with Children procedures and this policy should be read in conjunction with these procedures. These procedures outline the action that will be taken when there are concerns raised regarding someone's suitability to work with children, with regard to this policy it will specifically relate to concerns regarding contact, conduct or content on the Internet by people who work with children.

4.7 The use of personal mobile devices logged onto the council's guest wireless network are also subject to this policy e.g. smart phones, tablet devices etc.

5.0 Social media guidance

5.1 The council's Communications team operates a number of corporate social media accounts (e.g. Facebook, Twitter etc.)

5.2 The council provides business units and service areas with access to additional social media accounts to promote their services, engage with the public or businesses and to generate local discussion. Wherever possible these activities should be aligned with the council's website, corporate social media accounts and other offline communications.

5.3 Once the Head of Communications has granted authorisation, your manager should contact the IT Solution Centre in order to gain access to the appropriate social media sites. IT Services will keep a record of authorised users and ensure that before access is provided you have completed the 'Getting started with social media' e-learning module.

5.4 Council social media accounts must have strong passwords, which are changed regularly in accordance with the council's Information Security policy.

5.5 All employees using social media are reminded that they are personally responsible for anything they say online. They must also ensure that their use remains within legislation.

5.6 All employees using social media should be aware 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 is restricted to your 'friends'/'followers' it is in effect public as you cannot control what they do with any information you post.

5.7 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.

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

5.9 You should follow these guiding principles when using social media in your own time:

- You should not identify the council when using social media in a personal capacity if doing so would bring discredit to the council. This is a breach of the council's Disciplinary procedure and may result in action being taken against you.
- 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, e.g. 'these views are my own and do not necessarily represent the views of North Lincolnshire Council', if you have identified the council as your employer.

5.10 The council's facilities (e.g. Blackberrys, Internet etc.) must not be used to access personal social media accounts at any time.

6.0 Mobile device guidance

6.1 IT Services, on behalf of the council, is responsible for minimising the expenditure on mobile devices. Requests for a mobile device must be submitted via the online e-form. IT 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 (e.g. landline or email) are unsatisfactory.
- The employee's role involves out of hours support (e.g. 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. 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/corporate requirement for a mobile device (e.g. Emergency Planning).

6.2 IT Services will review the business case, submitted via an e-form, to ensure that there is sufficient evidence to support the request.

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

6.4 Any employee who is allocated a council mobile device must adhere to the content of this policy.

6.5 All council issued mobile devices with internet access (e.g. smart phones and tablets) are centrally managed. This includes the ability to remotely wipe lost or stolen devices and anti virus software where required.

- When using a council mobile device you must not call directory enquiries, that is any number which commences with 118 e.g. 118 118,118 247 etc. 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 IT Services (e.g. remote management, anti virus etc.)
- Install any software applications including the use of vendor 'app' stores (e.g. use of Google play store or Apple store etc.)

6.6 The authority may withdraw mobile devices at any time if it is found that the criteria for issue are no longer met, health and safety concerns arise or where there has been recognised misuse of the phone.

6.7 Use of council mobile devices for personal use is at managers' discretion. However, using a council mobile device for personal use should be kept to a minimum. .

6.8 It is an offence to use a mobile device, which is not fitted with hands free equipment whilst driving. You must not use a hand held mobile device whilst driving. Acceptable hands-free equipment relates to only manufacture installed and loud-speaker systems. Hands-free equipment that requires the use of a headset is not acceptable.

6.9 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 or earlier if requested to do so

6.10 In the event that the employee fails to return the mobile device, the employee's manager must inform the IT Solutions Centre as soon as possible, in order to ensure the connection is suspended.

6.11 Should an employee fail 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.

6.12 Personal mobile devices must not be used in connection with council business other than in accordance with section 7.0 of this policy.

6.13 Use of personal mobile devices in the workplace is subject to managers' discretion although, where use is permitted; this should be kept to a minimum and ideally restricted to breaks.

6.14 Personal mobile devices can be used to make business calls. The council will not refund any business calls made unless they are authorised by the relevant Director.

7.0 Use of personal devices

7.1 Personal devices of employees may be used to access council applications, its network and email. This is only possible when the device is configured to act as a proxy corporate device. When this is acceptable to both the council and the employee, the employee's personal device will have a secure workspace installed and integrated with the council's mobile device management system. This is currently Blackberry Enterprise Service 10 (BES 10). It allows the control of a range of operating systems, including, Windows, Apple, Blackberry and Android.

7.2 BES 10 has the capability to control personal devices. This includes wiping all data from them, both corporate and personal. The council respects the privacy of its employees and as such will only control the corporate workspace installed on employee's personal devices.

7.3 Without the permission of the employee the council will carry out the following functions:

- View a device report. This includes details such as the device name, operating system and serial number.
- Delete corporate data from the device.
- Lock the corporate workspace.
- Disable the corporate workspace.
- Review and interrogate the communications log. This will only be done for trouble shooting, support purposes or for event/incident investigations.

7.4 Only with the express permission of the employee (and on each occasion) will the council carry out the following functions:

- Specify the device password and lock.
- Lock the device.
- Unlock and clear the device password.
- Delete all device data.

7.5 If the employee's personal device is lost or stolen they must report this to IT Services as soon as possible. In such cases, or if the employee leaves the organisation, the council will remotely delete the corporate workspace.

7.6 Employees must use the corporate workspace in the same way as they would on any corporate device and fully comply with this policy.

7.7 The council does not provide any support for employees' devices, only the corporate workspace installed on them.

7.8 The use of an employee's device for business use, accessing the council's system and the installation of the corporate 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.

8.0 Access or removal of access to digital technologies

8.1 Managers should contact the IT Solution Centre in order to request access to any digital technology for their employees. They will need to provide details of what is required along with details of the business need.

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