

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 new Digital Technologies policy.

2. BACKGROUND INFORMATION

- 2.1 The council previously had four separate policies which governed employee use of the following digital technologies:

- Email
- Internet
- Social media
- Mobile phones

These four existing policies have been combined and streamlined whilst still providing a robust framework for managers and employees.

- 2.2 The policy is essential in governing how employees use digital technologies. 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.

3. OPTIONS FOR CONSIDERATION

- 3.1 To approve the new policy.
- 3.2 To reject the new policy.
- 3.3 To recommend amendments to the new policy.

4. ANALYSIS OF OPTIONS

- 4.1 Accepting the policy will ensure that employees are clear on what is expected of them when they are utilising digital technologies.
- 4.2 Rejecting the policy would result in a lack of clarity.

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

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

5.1 Financial

A separate report was recently submitted to CMT to seek approval for the centralization of mobile phone budgets in a bid to reduce costs.

5.2 Staffing

None.

5.3 Property

None.

5.4 IT

The IT controls outlined in the policy are already in existence.

6. OTHER IMPLICATIONS (STATUTORY, ENVIRONMENTAL, DIVERSITY, SECTION 17 - CRIME AND DISORDER, RISK AND OTHER)

6.1 An integrated impact assessment has considered the diversity implications of this policy.

7. OUTCOMES OF CONSULTATION

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

8. RECOMMENDATIONS

8.1 That the policy is approved and adopted.

ASSISTANT DIRECTOR HUMAN RESOURCES

Civic Centre
Ashby Road
SCUNTHORPE
North Lincolnshire
DN16 1AB
Author: R Stanford
Date: 20 December 2012

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
 - Social media
 - Mobile phones
- 1.2 This policy will be reviewed regularly to ensure that it remains relevant and also that any additional 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 ask that your manager email the IT Servicedesk in the event of a forgotten password, passwords cannot be acquired over the phone.
 - Should inform the IT Servicedesk if you believe there has been a breach of IT security.
 - 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 portable/mobile devices (e.g. Blackberry/iPad users) and if you access your council email account using your personal Apple iPhone or Android smart phone using the council's iTraveller solution.
- 3.2 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 Servicedesk 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 mail.
- Send email messages using another person's email account.
- Send unnecessary attachments, use document links as an alternative.
- 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.

3.3 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 you 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 Servicedesk.

3.4 All generic email accounts must be accessed via an employee's individual email account as part of Government Connect CoCo Compliance. If you are emailing

confidential information outside the council you must encrypt your messages to make them and any attachments secure.

- The Government Connect Gcsx 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 Servicedesk for these facilities to be set up on your account.

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

3.6 Personal email accounts must not be used for council business.

3.7 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 guidance

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

4.2 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 (inc. software, MP3 or other audio/video); illegal websites; personal networking and storage; peer to peer sharing; online gaming or malicious websites (eg. 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 Servicedesk, 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. The council operates the Managing Allegations Against People who work with Children procedures and this policy should be read in conjunction with these procedures.
- 4.6 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.

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 directorates 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 (e.g. Direct magazine).
- 5.3 Once the Head of Communications has granted authorisation, your manager should contact the IT Servicedesk in order to gain access to the appropriate social media sites. IT 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 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.

- 5.5 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.
- 5.6 You should follow these guiding principles for any social media activities that are part of your work:
- Be responsible for your actions
 - Be respectful
 - Be responsive
 - Be credible and consistent
 - Be legal
- 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 invoke 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 legal framework 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 phone guidance

6.1 Managers must be satisfied that one or more of the following business criteria are met, before authorising the issue of a mobile phone:

- The employee is a remote worker and requires a mobile phone to enable them to undertake their job effectively.
- Issuing the employee with a mobile phone 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 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 phone. A mobile phone 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 phone (e.g. Emergency Planning).

6.2 Any employee who is allocated with a council mobile phone will be required to complete and sign a declaration adhering to the content of this policy prior to the issue of the handset (See Appendix 1).

6.3 When using a council mobile phone 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.
- Leave a mobile phone ringing or unattended as this can cause a disturbance to other employees. Where practicable mobile phones should be set to silent mode, particularly in meetings, training etc.

- 6.4 The authority may withdraw mobile phones 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.
- 6.5 Use of council mobile phones for personal use is at managers' discretion. However to satisfy Internal Audit and Her Majesty's Revenue and Customs (HMRC) all employees are required to complete a declaration form for each bill they receive to identify and pay for any personal calls or to provide a nil submission if no personal calls have been made. (See Appendix 2).
- 6.6 It is an offence to use a mobile phone, which is not fitted with hands free equipment whilst driving. You must not use a hand held mobile phone whilst driving on council business.
- 6.7 Mobile phones provided by the council remain the property of the council. When an employee leaves the council it is the responsibility of the authorising manager and the employee to ensure that the mobile phone is returned. All personal charges plus VAT must be recovered from the employee prior to the leave date or as soon as possible thereafter.
- 6.8 Should an employee fail to return the mobile phone to the council they will be held responsible for any usage and line rental incurred until the mobile phone 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 and rental costs plus VAT.
- 6.9 Use of personal mobile phones 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.
- 6.10 Personal mobile phones should not normally 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 Access or removal of access to digital technologies

- 7.1 Managers should contact the IT Servicedesk 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.
- 7.2 If access to any digital technology is no longer required the employee's manager should contact the IT Servicedesk.

Declaration of use of council owned mobile phone.

Name: _____ Directorate: _____
Job title: _____ Payroll number: _____

Mobile phone no: _____

I certify that:

- I have been issued with a copy of the Digital Technologies policy, which I have read, understand and will comply with.
- I agree to return the mobile phone when leaving the employment of the council or earlier should a request be made in accordance with the policy.
- I agree to repay the costs of all my personal calls and text messages and acknowledge that I may be liable for costs relating to loss and/or damage due to my own negligence and any costs arising from the non–return of the mobile phone in accordance with the policy.
- I understand that I may be liable to disciplinary action should I fail to comply with the policy.

Employee

Signed: _____
Date: _____

On behalf of IT Services

I confirm that I have issued the above mobile phone to the above employee.

Signed: _____ Print name: _____
Date: _____

Declaration of the personal use of council owned mobile phones.

It is a requirement of Internal Audit and Her Majesty's Revenue and Customs (HMRC) that all users highlight their personal calls and ensure that the amount, plus 20% VAT is paid.

Name: _____ Directorate: _____
Job title: _____ Payroll number: _____
Mobile phone no: _____ Bill period: _____

Total personal calls/texts
VAT at 20%
Total amount to pay

I certify that I have identified all personal phone calls and text messages above and that the remaining calls were made on council business.

Please pass this completed form to your line manager; it will be retained for audit purposes

Cost code*
Expense code
Job reference

**Please look on your statement in the left hand corner next to your name.*

If there are no personal calls, please submit this as a nil return.

Signed: _____
Date: _____