Information Security Document

Acceptable Use of Internet, Email and Social Media Policy

Version 9.0

Version History			
Version	**Date**	**Detail**	**Author**
1.0	23/06/2004	Approved for distribution	Human Resources & UNISON
2.0	27/09/2011	Approved by Information Governance Group	Jo White
3.0	31/10/2012	Reviewed by Information Governance Group	Jo White
4.0	10/02/2014	Reviewed by Information Governance Group	Jo White
5.0	12/01/2015	Reviewed by Information Governance Group. Updated with ISO27001:2013 controls and removal of Derbyshire email for personal use.	Jo White
6.0	10/10/2016	Reviewed by Information Governance Group. Compliance with Secure Email Policy for external recipients added.	Jo White
7.0	08/01/2018	Reviewed by Information Governance Group. Transformation changed to ICT.	Jo White
8.0	04/03/2019	Reviewed by Information Governance Group. Incorporation of Skype Acceptable Use Policy.	Jo White
9.0	18/12/2019	Reviewed by Information Governance Group. Social Media Policy merged in to Internet Policy. Addition of email photos and ePayslips.	Jo White

This document has been prepared using the following ISO27001:2013 standard controls as reference:

ISO Control	Description
A.8.1.3	Acceptable use of assets
A.7.1.2	Terms and conditions of employment
A.12.1.3	Capacity management
A.13.2.3	Electronic messaging
A.12.4.1	Event logging
A.16.1.7	Collection of evidence
A.18.1.2	Intellectual property rights

1 Introduction

Derbyshire County Council's reliance on the use of the Internet, email and social media is essential to the effective delivery of the services it provides. Along with this reliance, comes the need to identify and address the vulnerabilities and risks associated to ensure that we are protecting every aspect of the Council's business and are able to maintain the efficient and effective services to both our service users and the general public.

2 Purpose

The purpose of this policy is to provide clear guidance on acceptable behaviour in the use of the Internet and email - including the use of social media both during and out of work and that it is consistent with the Council's Employee Code of Conduct, Acceptable Use policies, Risk Management Strategy and professional best practices. Nothing in this policy should be read as restricting the proper use of Internet, email and social media for work purposes.

3 Scope

This policy applies to all employees, elected members, contractors, volunteers, vendors, apprenticeships, student/work experience placements and partner agencies who have access to use the Council's Internet and email and who use both work and/or personal social media and internet related accounts where they may also be representing the Council by virtue of association such as that of an employee.

This policy applies to all information technology and communications equipment provided by the Council capable of accessing the Internet, sending/receiving emails and of using social media accounts e.g. PC's, laptops, tablets, mobile phones and all other internet capable computing devices.

4 Policy Statement

All parties identified in the scope of this policy are required to maintain the good reputation of the Council when using the Internet, email and social media. Any such use which brings the Council into disrepute may result in removal of internet, email and Council social media access and disciplinary action may be taken against employees where necessary.

Any personal information sent via email, the Internet, social media and associated services such as Skype, is covered by the Data Protection Act 2018. All parties are required to handle personal information in accordance with the Data Protection Act and the GDPR. Further information about handling personal data is available in Derbyshire County Council's Safe Haven Guidance:
https://www.derbyshire.gov.uk/working-for-us/data/importance-of-data-security/importance-of-data-security.aspx

5 INTERNET USE

For the purpose of this policy, the use of the internet will include associated internet enabled technologies such as Skype.
Use of the Council's internet systems is restricted to the following conditions:

- Personal use of the Internet is not allowed during working hours.
- Personal use is only permitted in your own time and limited to browser based activities. You can use the Internet before you start work, during your lunchtime, or after work. For flexi-time users this should be recorded accordingly in Workplace as non working time.
- Any personal use must not, in any way, distract others from the effective performance of their duties. Improper or inappropriate personal use of the Council's Internet and associated systems may result in disciplinary action.
- You must not use the Council's Internet systems for trading or personal business purposes.
- You must not reveal personal, sensitive or confidential information relating to service users or the Council.
- You are advised not to conduct online payments. This is due to the information being stored locally on your computer, which potentially could be compromised, putting the user at financial risk. If you use the Internet to buy goods or services, the Council will not accept liability for default of payment or for security of any personal information you provide. Goods must not be delivered to a Council address.
- All Internet sessions should be terminated as soon as they are concluded.
- Use of Council Skype services for personal use is not permitted at any time. More information on the use of other social media can be found in section **8 Social Media Use** of this policy.
- Consent must be obtained for any recordings of conversations resulting from the use of facilities such as Skype.
- Desktop and document sharing capabilities of facilities such as Skype, must only be used with colleagues and partners of the Council for collaboration purposes. If you allow changes to be made to these documents during a desktop sharing session, as the 'sharer' of the document, it is your responsibility to ensure that the documentation is used correctly and saved appropriately.
- You must use the Council's internet provision responsibly in accordance with this policy and all relevant policies and guidelines.

5.1 Filtering Content

Many Internet sites that contain unacceptable content are blocked automatically by the Council's systems. However, it is not possible to block all "unacceptable" sites electronically in all circumstances.

The Council has a process in place to block categories of internet sites and individual sites if it is deemed appropriate to do so.

5.2 Downloading Material

- Downloading of video, music files, games, software files and other computer programs is not permitted. These types of files consume large quantities of storage space on the system (and can slow it down considerably), may violate copyright laws

and may pose serious security risks by introducing malware/viruses onto the Council's computer network.

- Online Mapping Software should not be used unless for specific work purposes as it is resource intensive and involves downloading an application to your computer.
- Streaming media, such as radio or tv programmes, for non-work related purposes is not permitted.

If you are in doubt about software use or installation, seek guidance from the Council's ICT Service.

5.3 Accidental Access To Inappropriate Material

You may receive an email or mistakenly visit an Internet site that contains unacceptable material. If this occurs, you must inform your line manager or a more senior manager immediately. Your manager will ask you for details relating to the incident and you will be asked how the event occurred. This information may be required later for management and audit purposes.

5.4 Copyright

You may be in violation of copyright laws if you simply cut and paste material from one source to another. Most sites contain a copyright notice detailing how material may be used. If you are in any doubt about downloading and using material for official purposes, you should seek advice from the Council's Legal Services Division.

6 EMAIL USE

Email is an extremely efficient means of communication but always ask yourself whether a quick internal telephone call would be more effective than sending an email message.
Use of the Council's email systems is restricted to the following conditions:

- Personal use of derbyshire.gov.uk email or any other email system provided for use as a Derbyshire County Council employee, is not permitted at any time. It is also inappropriate as it may give the impression that any business is on behalf of the Council.
- If a genuine emergency arises where you have received and replied to email for personal reasons, you should inform your line manager at the earliest opportunity that you have responded to the email and they will make a note of it. You should inform the sender that personal use of the Council's email system is not permitted and an alternative method of communication will need to be considered.
- Emails should only be kept in your inbox for a maximum of 6 months. Any emails that you need to keep beyond this period should be moved to appropriate file storage, EDRM or network files.
- You must only use Council provided email systems to send and receive Council information.
- Employees are permitted to send their copy payslips to a personal email account. This must be done in compliance with the Council's Secure Email Policy.
- You must not use the email system in any way that is insulting or offensive - as described in section **9 Unacceptable Use.**

- Any authorised personal data sent externally by email e.g. to solicitors, Inland Revenue etc must be sent in compliance with the Secure Email Policy: https://www.derbyshire.gov.uk/working-for-us/data/sharing-information/sharing-information.aspx
- You must not use anonymous mailing services to conceal your identity when mailing through the Internet, or falsify (spoof) emails to make them appear as if they have been sent from someone else.
- All emails are automatically tagged with the classification 'controlled'. You should consider whether you need to change the classification to 'public' or 'restricted'.
- If you receive an email that is inappropriate or abusive, you must report it to your line manager immediately, who will take the appropriate action. If the sender is known to you, inform them that they should cease sending the material.
- Emails which appear suspicious, may be 'phishing' or malware attempts, must be reported immediately as a security incident in accordance with the Council's Security Incident Management Policy and Procedures: https://www.derbyshire.gov.uk/working-for-us/data/if-something-goes-wrong/report-a-security-incident.aspx

The content of incoming email is automatically scanned to detect computer viruses, however, the actual text of the email is not viewed as part of this process. The content of all emails may be viewed by the Council in certain circumstances; for example, in connection with disciplinary investigations or Audit reviews.

See guidelines on email management for advice on email etiquette: https://www.derbyshire.gov.uk/working-for-us/data/at-your-desk/email/internet-and-email.aspx

6.1 Email Disclaimer

A disclaimer is automatically attached to all emails sent from the Council informing the recipient that the email is intended solely for them, is confidential, may be legally privileged and may contain personal views that are not those of the Council.

6.2 Office 365 Photos

Staff can voluntarily choose to have a photo assigned to their Office 365 account. The stored photo linked to ID badges may be used if available. Alternatively, staff are permitted to upload one of their own choosing, provided it conforms to the following criteria:

- a recognisable recent image of yourself
- suitable for a professional environment
- close up of face, head and shoulders
- free from reflection or glare on glasses
- contain no other subjects in the photo
- of a file size smaller than 4MB
- of file format .png, .jpg or .gif

No other images are acceptable including icons or caricatures.

6.3 Access To Email

Where an employee is absent, the employee's line manager may authorise access to a

Council email account to obtain messages which require an action during their absence. The manager will inform the employee of this access on the employee's return.

For setting up delegates to access your inbox on a permanent basis, please see: https://www.derbyshire.gov.uk/working-for-us/data/at-your-desk/email/internet-and-email.aspx

7 INSTANT MESSAGING (IM) USE

Instant Messaging is a form of real time communication between two or more people based on typed text. The text is conveyed via devices connected over the Internet or an internal network/intranet. Messages are retained in your conversation history in your email folder list or are saved as emails in your inbox if the recipient does not respond immediately.

You must only use Council provided internet messaging (IM) services.
IM should not be used as a substitute for email. IM should be used only for questions or announcements that are short and need to be communicated immediately.
Private use of instant messaging for any purpose is not permitted.

8 SOCIAL MEDIA USE

Social media is a type of interactive online media that allows parties to communicate instantly with each other, or to share data in a public forum. This includes online social forums such as Twitter, Facebook, Linked-In, internet newsgroups, and chat rooms. Social media also covers blogs and video/image sharing websites such as Instagram, YouTube and Flickr. There are many more examples of social media than can be listed here and this is a constantly changing area. This policy refers to all social media, including the examples listed, and any new social media which is developed in the future.

The Council recognises that the Internet provides an opportunity to participate in interactive discussions and share information using a wide variety of social media. The scope of this policy applies to those who are likely to use social media privately, (outside of work) as well as in their role during office hours or otherwise - whether the social media is accessed using Council ICT facilities, or by using personal equipment where they may be representing the Council such as that of an employee.

Use of social media is restricted to the following conditions:

- All employees are expected to behave appropriately and responsibly, and should be aware that they may be accountable to the Council for actions outside of their work.
- An employee's personal social media account should not, directly or by implication, give the impression that they are endorsed by, or speaking on behalf of the Council.
- Online conduct is the employee's responsibility, and it is important that employees are aware that posting information on social networking sites in a personal capacity cannot be entirely isolated from their working life.
- Any information published online can be accessed around the world and will be publicly available for all to see, and this may be impossible to delete / withdraw

once published.

- You should not upload images or video files of work based activities unless authorised by your line manager.
- The Council views any comment that is made on a social media site to have been made publicly, and that any inappropriate comment made, will be considered in the context of which it is made.
  For example, disparaging comments against a colleague made on Facebook could be viewed as bullying/harassment, and could be considered to bring the Council into disrepute.
- Employees should be aware that all comments made through social media must meet the standards of the relevant legislation and regulations, including Data Protection legislation, the Employee Code of Conduct and the Equality and Diversity policy.
- Employees may be accountable for actions outside of work, including making comments on social media sites, if that is contrary to any of Council's policies and procedures, impacts on or compromises the employee's ability to undertake their role, or undermines management decisions. Such behaviour could be investigated and may result in disciplinary action and ultimately could result in dismissal.

Further employee guidance is available in Appendix A

8.1 Access To Social Media For Work Purposes

Employees who use social media as part of their job must adhere to this Policy. Employees must be aware that they are representing the Council when they are contributing to the Council's social media activities. Employees should use the same safeguards as they would with any other form of communication about the organisation in the public domain.

8.2 Access To Social Media At Work, For Personal Use

Employees are not allowed to access social media websites for personal use from the Council's computers or devices during working time and they must not be left constantly running 'in the background', whilst at work. These provisions also apply to personal computers and mobile devices.

Employees' use of social media in both a personal and business capacity can present risks to the Council's information and reputation, and can jeopardise our compliance with legal and statutory obligations. To minimise these risks, and to ensure that our ICT resources and communications systems are used appropriately, employees must comply with this policy.

8.3 Personal Safety And Privacy

Employees need to be aware that the information they post on their personal social media profile can make them identifiable to service users, as well as people they know in a private capacity.

Employees should therefore consider this when setting up their online profile particularly in relation to; use of a photograph, providing details of their occupation, employer, and work

location.

Employees should ensure that clients known to them through their work, *where there could be a conflict of interest*, are not linked to them through social media. The Council considers it inappropriate to have service users as 'friends' through social media, especially where these people are vulnerable and there may be safeguarding issues.
For example, it would be inappropriate for Social Workers to have service users and their families as 'friends' on Facebook.

Online sites such as Facebook are in the public domain, and personal profile details can be seen by anyone, even if users have their privacy settings on the highest level. Also if a user's profile is linked to other sites, any changes to their profile will be updated there too. Employees who have set their privacy level to the maximum can have their privacy compromised by 'friends' who may not have set their security to the same standard.

9 UNACCEPTABLE USE

These conditions apply to all internet, email and social media use as identified in this policy.

You must not deliberately view, copy, create, publish, download, save, print, participate in or distribute any material that:

- is sexually explicit or obscene.
- includes discriminatory, derogatory or offensive, inappropriate comments, media or images relating to sex, sexual orientation, gender, reassignment, disability, age, religious belief, nationality or race – including links to such materials.
- contains material the possession of which would constitute a criminal offence.
- promotes or participates in any form of criminal activity.
- contains unwelcome propositions.
- involves gambling, multi-player games or soliciting for personal gain or profit.
- contains images, cartoons or jokes that may cause offence.
- appears to be a chain letter.
- knowingly misrepresents and/or brings the Council into disrepute or exposes it to legal action.
- contains defamatory comments, images or media about individuals or other organisations / groups and that which could also be considered as bullying or harassment.
- agrees with or condones inappropriate comments or content.
- contains or refers to confidential and/or personal information about an individual, such as a service user, colleague or the Council.

Employees are encouraged to talk to their manager and seek advice if they are unclear.

Managers should ensure that all reports of inappropriate use and/or complaints are dealt with consistently, fairly and in a timely manner.

All employees are required to make themselves aware of the Council's Information Security policies. See the 'Data Security' section of working for us on the Council's

website: www.derbyshire.gov.uk/data

This policy should be read in conjunction with the Employee Code of Conduct, Harassment and Bullying Procedure, ICT Acceptable Use policy and Media Contact policy.

The Council reserves the right to withdraw Internet access, email or social media use - including access to the Council's computer or communications network, if the user has been found to be in breach of these conditions.

This list is not exhaustive and the Council may define other areas of unacceptable use.

10 MONITORING

The Council maintains logs of all internet, Skype, instant messaging (IM) and email use and monitors the service constantly

10.1 Monitoring Internet Access

Derbyshire County Council records the details of all Internet traffic. This is to protect the Council and its employees from security breaches, including hacking, and to ensure that "unacceptable" sites are not being visited.

The logs record:

- the network identifier (username) of the user,
- address of the Internet site being accessed,
- where access was attempted and blocked by the system,
- the Web page visited and its content,
- the name of any file accessed and/or downloaded,
- the identity of the computer on the network and the date and time.

Any excessive or inappropriate use may result in disciplinary action being taken.
All monitoring information will be kept for six months.

10.2 Monitoring Of Email And Instant Messages

The Council's email system automatically records details of all email sent both internally and externally. The automatic system highlights the use of certain prohibited words and any potential infringement will be referred to Executive Directors by Audit Services as part of routine audit reviews.

The following details are recorded in respect of every email message:

- name of the person sending the email,
- the email addresses of all recipients and copy recipients,
- the size and name of any file attachments,
- the date and time sent,
- a copy of the email,
- a copy of file attachments.

The Council may read and inspect individual emails and attachments for specific business purposes or during disciplinary investigations including:

- Establishing the content of transactions,
- Ensuring employees are complying both with the law and with the Council's email policy, and
- Checking email when employees are on leave, absent or for other supervisory purposes.

The Council routinely produces monitoring information, which summarises email usage and may lead to further enquiries being undertaken.

Monitoring information will be kept for six months.

Emails, including conversations recorded using facilities such as Skype, are covered by the Freedom of Information (FOI) Act and may be disclosed as part of an FOI request for information, or as part of any legal proceedings. Always exercise the same caution on email content as you would in more formal correspondence.

BREACHES OF POLICY

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Council assets, or an event which is in breach of the Council's security procedures and policies.

All employees, elected members, contractors, volunteers, vendors, apprenticeships, student/work experience placements and partner agencies have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Council's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Council.

The Council will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an individual, then the matter may be dealt with under the disciplinary process.

It is your responsibility to read this policy carefully and to ask your line manager to explain if there is anything you do not understand. If you feel you may have accidentally breached this policy, you should contact your line manager **immediately**, or, in their absence, a more senior manager who will record this information. See **9 Unacceptable Use**.

Further Information

An Employees' Guide to the Acceptable Use of Social Media and Derbyshire County Council Social Media Protocols are attached in **Appendix A** and **Appendix B**.

This policy also works alongside other policies and procedures including;

- ICT Acceptable Use Policy
- Employee Code of Conduct
- Disciplinary Procedure
- Harassment and Bullying Procedure

- Social Media Protocols
- Media Contact Policy

Copies of all policies and procedures are available on the Council's website, www.derbyshire.gov.uk/data or from your manager.

This document is owned by the Information Governance Group and forms part of the Council's ISMS Policy and as such, must be fully complied with.

APPENDIX A

EMPLOYEE GUIDANCE ON THE ACCEPTABLE USE OF SOCIAL MEDIA

- Employees must be mindful that any online activities/comments made in a public domain, must be compatible with their position within the Council, and safeguard themselves in a professional capacity.
- Protect your own privacy. To ensure that your social network account does not compromise your professional position, ensure that your privacy settings are set correctly.
- Comments made outside work, within the arena of social media, do not remain private and so can have an effect on or have work-related implications. Therefore, comments made through social media, which you may intend to be "private" may still be in contravention of the Employee Code of Conduct, the Harassment and Bullying procedure and / or the Disciplinary procedure. Once something is online, it can be copied and redistributed making it easy to lose control of. Presume everything you post online will be permanent and can be shared.
- Do not discuss work-related issues online, including conversations about service users, complaints, management or disparaging remarks about colleagues or the Council. Even when anonymised, these are likely to be inappropriate. In addition doing this in the presence of others may be deemed as bullying and/or harassment.
- Do not under any circumstances accept friend requests from a person you believe could be a service user or may conflict with your employment.
- Be aware that other users may access your profile and if they find the information and/or images it contains offensive, make a complaint about you to the Council as your employer.
- Ensure that any comments and/or images cannot be deemed defamatory, libelous or in breach of copyright legislation.
- When setting up your profile online consider whether it is appropriate and prudent for you to include a photograph, or provide occupation, employer or work location details.
- You can take action if you find yourself the target of complaints or abuse on social networking sites. Most sites will include mechanisms to report abusive activity and provide support for users who are subject to abuse by others.
- If you do find inappropriate references and / or images of you posted by a 'friend' online you should contact them and the site to have the material removed.
- If you are very concerned about someone else's behaviour online, you should take steps to raise your concerns. If these are work related you should inform your manager.
- Employees should also act in accordance with the Council's Employee Code of Conduct, Internet and Email Acceptable Use procedure, Acceptable Use of ICT policy and Harassment and Bullying procedure.
- Employees should not access social media sites or leave these running in the background during working time, *for personal use*, on any devices within their control.

APPENDIX B

DERBYSHIRE COUNTY COUNCIL SOCIAL MEDIA PROTOCOLS

Purpose

Derbyshire County Council social media accounts should be used to promote council policies, events and services. They should not be used to promote the views, opinions or experiences of individual officers.

Account Creation

Creation of all county council social media accounts needs to be approved by the digital manager, working in the communications divisions. Individual officers cannot have county council social media accounts in their own name.

Approval

Departmental, service and project social media accounts need approval of the digital manager before set-up. A brief business case must be provided for each proposed new social media profile. A proposal form can be found on Dnet or via the Digital Communications Team, it includes:

- Why the account is needed
- Who it is aimed at
- Key objectives and messages
- Who will manage the account and post content
- How often it will be used and reviewed against its objectives
- An exit strategy for closing the account if it doesn't meet its objectives

Elected Member Accounts

Elected members can set up their own social media accounts which are hosted externally. Links to them can be included on the elected member's page on the county council website.

Personal Accounts

Social media accounts held by officers in their private capacity should avoid commenting on council policies and any other issues relating to their position within the council. For further guidance see the Acceptable Use of Social Media Policy.

For Further Advice:

Digital Communications Team

01629 539244 econtent@derbyshire.gov.uk