Medway Council
Internet, E-mail and Social Media Policy and Guidelines

Issue Date: November 2014
Review Date: November 2016

Lead Officer: Carrie Mckenzie, Head of HR and Organisational Change

Table of Contents

Medway Council Internet, Email and Social Media Policy and Guidelines

1. Aim of this Policy

1.1 This Policy and guideline document “the Policy” has been produced to help employees and managers understand their responsibilities when using the Internet, e-mail and social media. They are not designed to deter employees from using these communication tools but are necessary to help protect employees and prevent them from bringing the council into disrepute either inadvertently or intentionally and the potential consequences of doing so.

1.2 “The Policy” applies to all Medway Council employees, including those in local authority, community, special, and voluntary controlled schools and those who work as partners with Medway Council.

1.3 All existing authority policies apply when using the Internet, e-mail and social media e.g. data protection, whistle blowing, dignity at work (bullying and harassment), disciplinary, employee code of conduct and client confidentiality.

1.4 All employees should be aware that failure to follow the detail within “The Policy” will be regarded as a breach that may lead to actions as detailed in **Section 6.**

2. Use of Internet, e-mail and social media - principles

2.1 Use of the Council Internet and email system and/or equipment is strictly for employees use only (or other authorised personnel) and is primarily for business use only

2.2 Occasional and reasonable personal use e.g. online shopping, social media, websites etc is permitted outside of core working hours only. Responsibility for ensuring compliance lies with the line manager. Employees continually abusing this may be subject to disciplinary action.

2.3 The use of the Internet to make negative or defamatory comments about Medway Council or its officers or members will be regarded as a breach of “The Policy” that will usually result in disciplinary action and may also result in potentially legal action on a collective or individual basis (see also Section 6). Employees should speak to their line manager if in any doubt~~.~~

2.4 The principles within “The Policy” covers all electronic communication tools but the primary focus is on the use of Internet, e-mail and social media. They provide guidelines on what employees should and should not do and help to:

- Develop good practice;
- Maintain council system's security and protect it from viruses, and
- Prevent misuse.

2.5 Line managers are responsible for ensuring that employees under their management are made aware of “The Policy” prior to using the council’s Internet or e-mail systems.

3. Internet and Intranet systems

3.1 The following conditions cover the use of the Internet and Intranet, and apply to:

- Any equipment owned (or made available to you) by Medway Council, at any location.
- Any Medway Council systems accessed on home equipment.

3.2 Although software is available for download from a variety of Internet sites, no such software must be downloaded onto Medway Council equipment. Only Corporate ICT staff are authorised to download software onto Medway Council equipment, as required for essential and approved software installations.

3.3 No alternative Internet Service Provider (ISP) should be installed and used on any equipment belonging to Medway Council. Access to the Internet should be via the Medway Council connection only.

3.4 Employees must not send unsolicited, irrelevant or inappropriate e-mail to multiple newsgroups or any mailing lists on the Internet.

3.5 Use of the Internet and/or council equipment to access, propagate or store pornography, material of a sexual or illegal content or any material which could be offensive or lead to accusations of harassment (including jokes), is strictly prohibited. In addition, employees should not use the Internet to propagate any computer games, illegal file sharing or other software, which could be considered an abuse of the council's time and resources.

3.6 Internet usage and sites visited will be monitored and any unauthorised or inappropriate use is prohibited. In the event that an employee accidentally or through a computer virus unintentionally accesses any site(s) or data as suggested in paragraph 3.7, the employee should immediately inform their line manager who will liaise with ICT for advice.

3.7 Internet access is provided subject to the Medway Council ICT Security Policy and should not be used for any of the following:

- Breaking through security controls, whether on Medway Council equipment or on any other computer system;
- Intentionally accessing or transmitting computer viruses and similar software;
- Intentionally accessing or transmitting information about, or software designed for breaking security controls or creating computer viruses;
- Intentionally accessing or transmitting material which is obscene, sexually explicit, pornographic, racist, defamatory, hateful, incites or depicts violence or describes techniques for criminal or terrorist acts or otherwise represents values which are contrary to Council Policy;
- Political lobbying *unless your role particularly requires this, e.g. Political Assistants* or private business;
- Any activity which could cause congestion and disruption of networks and systems.

4. E-mail

4.1 Although the e-mail system is primarily for business use, occasional and reasonable personal use is permitted during non-working hours only. Responsibility for ensuring compliance is with the employees line manager.

4.2 Employees choosing to send a personal e-mail should start or sign off the e-mail with the following statement:

"This e-mail is personal. It is not authorised by or sent on behalf of Medway Council and is the personal responsibility of the sender."

Note: employees should be aware that a corporate footer is attached to every outbound e-mail.

4.3 All e-mail usage may be monitored and e-mail inspected (including personal email) at any time without notice.

4.4 Employees wishing to send e-mail to all council employees should contact ICT. This service is for business use only.

4.5 **Legal issues**

4.5.1 The contents of e-mails can be legally binding and may be produced in court as evidence. Employees must make sure that any messages sent by e-mail do not personally commit either themselves or the council to any action that has not already been agreed. Messages must not be derogatory or mis-represent other people or organisations. If employees are in any doubt they should speak to their line manager. A good test of appropriateness would be for an employee to ask themselves how they would feel if their message was read out in court.

4.5.2 No document or attachment may be e-mailed unless the employee has a legal right to distribute the document and it conforms to all legal requirements such as data protection and copyright. Employees who have any doubts should consult the legal department.

4.6 **Dealing with e-mail**

4.6.1 When dealing with e-mail employees should:

- Be aware that both internal and external e-mails are not guaranteed to be private and could occasionally not arrive at all. If delivery is important employees should make sure they get confirmation of receipt;
- Check for incoming e-mail on each working day or arrange for a duly authorised person to do so on their behalf;
- Have reasonable expectations about replies; remember that sending information or requests via e-mail does not necessarily give them priority to the recipient, in particular those who choose to send emails outside of normal working hours e.g. evening and weekends;
- Avoid sending unnecessarily long e-mails; convey important points first; put dates; deadlines and the purpose of the message in the first one to three lines of the message. Avoid bulky paragraphs wherever possible as this discourages reading.
- Be mindful not to send e-mails when it is not necessary. Think about whether it is necessary to e-mail "thank you" or other pleasantries on every occasion. This will

help prevent the recipients mailbox overloading and will also save them time opening unnecessary e-mails;

- Be selective as to who they copy e-mails into and endeavour to keep this to a minimum whenever possible. Employees should think about why they are copying people in and only do so if it is completely necessary. Those who choose to “blind copy” should do so with care.
- Select the e-mail title carefully; keep the title brief and think about what will increase the chances of readership;
- Ensure that they are sending the e-mail to the correct recipient; if the e-mail is sensitive and/or confidential double check before sending;
- Be mindful that e-mail is not always the best way to communicate.

4.7 **Misuse of e-mail**

4.7.1 Employees must not send unsolicited, irrelevant or inappropriate e-mail to multiple newsgroups or mailing lists on the Internet, nor should they participate in chain or pyramid letters or similar schemes.

4.7.2 Use of e-mail to propagate or store pornography, material of a sexual or illegal content or any material which could be offensive or lead to accusations of harassment (including jokes), is strictly prohibited. In addition employees should not use e-mail to propagate any computer games or other software which could be considered an abuse of the council's time and resources.

4.7.3 Employees must not;

- Use anonymous mailing services to conceal their identity when using e-mail;
- Falsify e-mails to make them appear to originate from someone else;
- Provide false information to anyone requesting name, e-mail address or other details.

4.8 **System security**

4.8.1 Viruses can be transmitted via e-mail. Employees must take care to make sure that all data sent or received is virus-free. If employees have any concerns when receiving external e-mail, including files received as e-mail attachments they should contact the ICT Service Desk on X2888 before opening them.

5. Social Media

5.1 Social media describes the online tools, websites and services that people use to share content, profiles, opinions, insights, experiences, perspectives and media itself. These tools include social networks, blogs, message boards, podcasts, microblogs, lifestreams, social bookmarking, wikis, and vlogs.

5.2 The feature that all these tools, websites and services have in common is that they facilitate conversations and online interactions between groups of people.

5.3 A few well-known examples of popular social media applications are Wikipedia (wiki), MySpace and Facebook (social networking), Twitter (microblog), YouTube (video sharing), Flickr (image sharing) and del.icio.us (bookmarking).

5.4 Social media has great potential to help the council reach residents that do not engage using traditional communications and engagement channels. However the inappropriate or ill-considered use of social media also has the potential to damage both individual's and the council's reputation. It is therefore important that staff are aware that there are a number of legal implications associated with the inappropriate use of social media. Liability can arise under the laws of defamation, copy-right, discrimination, contract, human rights, protection from harassment, criminal justice act etc. This list is however non-exhaustive.

5.5 Enquiries or requests for information from social media, including requests from bloggers, should be forwarded to the Communications and Marketing team for a response. Officers must not respond directly to such enquiries without express permission from the Communications and Marketing team.

5.6 Personal use of social media at the workplace and at home

5.6.1 This section of the guidelines provide guidance on the use of social media tools by council officers in a personal capacity. For example this includes a personal profile on Facebook or use of Twitter in a personal capacity by council officers. This includes personal use at work and at home.

5.6.2 Employees using the council's resources to access social media sites must ensure that their online activities do not interfere with their job, colleagues or commitments to customers. Occasional and reasonable personal use e.g. online shopping, social media, websites etc is permitted during non-working hours only. Responsibility for ensuring compliance is with the employees line manager.

5.6.3 When using social media, employees should respect their audience. As a general rule, employees should be mindful of any detrimental comments made about colleagues whilst using social media. Any conduct which breaches the employee code of conduct such as failing to show dignity at work (harassment), discriminatory language, personal insults, obscenity, disclosure of confidential information will be considered a disciplinary matter. These examples are not exhaustive.

5.6.4 Employees should also show proper consideration for others' privacy and for topics that may be considered objectionable or inflammatory – such as politics and religion.

5.6.5 Employees must be aware of their association with Medway Council when using social media. If they identify themselves as a Medway Council employee, they should ensure that their profile and any related content is consistent with how they would wish to present themselves with colleagues and customers.

5.6.6 Employees who may not directly identify themselves as a Medway Council employee when using social media for personal purposes at work or at home, should be aware that content they post on social media websites could still be construed as relevant to their employment at Medway Council. For example employees should not normally write or report on conversations, meetings or matters that are meant to be private or internal to Medway Council. Unauthorised disclosure of confidential information would constitute misconduct/gross-misconduct in accordance with the council's disciplinary policy. Employees should not cite or reference customers, partners or suppliers without their written approval. If it is necessary to make a reference, where possible link back to the source.

5.6.7 The council will not accept liability for any actions arising out of employee's personal use of social networking sites.

5.6.8 The council will monitor the use of social networking sites to ensure that any use by employees complies with its internet policy.

5.6.9 Additional guidance, produced by the Children and Adult's Directorate relating in particular to staff who have contact with clients and children is attached as Appendix 1.

5.7 Using social media for professional purposes

5.7.1 This section of the guidelines relate to the use of social media tools by council officers in the course carrying out their normal duties in delivering council services. For example this would include using a Facebook page to promote the council's Castle Concerts event or using Twitter to promote community safety initiatives.

5.7.2 Employees should not use any social media tool for Medway Council business without the appropriate authorisation, which is:

- Internally focused – a request should be made to the corporate communications group via the Employee Engagement Manager, HR Services;

- Externally focused, i.e. communications on behalf of Medway Council, council services or a partnership of which the council is a member – a business case should be made using the pro-forma (attached as Appendix Two) to the Communications and Marketing Team who will consider and refer to the appropriate Assistant Director/Deputy Director with their supporting advice for authorisation.

5.7.3 Employees should:

- Not use any social media tool for Medway Council business unless they have received appropriate training and are registered on the approved business social media user list held by the Communications and Marketing team;
- Identify themselves – this means disclosing their name and role at Medway – when discussing Medway Council or council related matters;
- Remember that they are personally responsible for the content they publish on blogs, wikis or any other form of user-generated media;
- Be mindful that what they publish will be public for a long time and can't be retracted once they are published;
- Not write or report on conversations, meetings or matters that are meant to be private or internal to Medway Council;
- Not cite or reference customers, partners or suppliers without their written approval. Where employees do make a reference, where possible link back to the source;
- Make sure that professional use of social media adds value to the environment in which they are participating and to the council's delivery of services to Medway residents;
- Provide worthwhile information and perspective;
- Be aware that content on such social media websites may be subject to Freedom of Information requests.
- Remember that Medway Council's reputation is heavily influenced by its people and what is published will reflect on Medway's reputation.

5.7.4 Anything posted should respect copyright and be consistent with the relevant legislation and rules including Data Protection Act 1998, Privacy and Electronic Communications Regulations 2003, ASA CAP code and the Code of Recommended Practice on Local Authority Publicity. It is the responsibility of the employee to make sure that they are familiar with how these apply to professional use of social media. If in doubt in the first instance employees should consult with their line manager.

5.7.5 Employees will be held personally liable for any un-authorised, inappropriate or illegal use of social networking sites.

6. Breach of Policy

Any breach of this policy may lead to disciplinary action and any serious breach will be regarded as Gross Misconduct which may lead to termination of employment.

A breach of legislation (such as detailed at 5.7.4) may lead to criminal or civil action being made against the individual(s) involved