CAMBRIDGE
CITY COUNCIL

EMAIL, INTERNET & SOCIAL MEDIA GUIDE

October 2018

To be reviewed October 2019

Contents

1. Our Approach

Cambridge City Council wants to ensure all employees are clear about acceptable and professional use of information technology. The use of social media can be a very effective means of communicating with our residents and professional networks. We want to maintain the council's reputation whilst utilising different ways of engaging with customers and staff and encourage you to behave responsibly online, both inside and outside of work.

It is the responsibility of all line managers to ensure that employees are working within the parameters of this guidance. Line managers are expected to provide details of this guidance in local induction processes and have evidence to show that employees are aware of this policy and their responsibilities.

This guide should be read in conjunction with the Code of Conduct, which outlines what is expected of employees in terms of maintaining the council's reputation and in your dealing with customers and colleagues; particularly in relation to political neutrality and personal integrity. There is a separate Councillor Code of Conduct for Councillors.

This guide applies to you if you carry out any work for Cambridge City Council, whether as an employee, temporary agency worker, casual, consultant, work experience student or volunteer. Cambridge City Council is committed to equality of opportunity and wants to ensure everyone is treated with dignity and respect irrespective of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex or sexual orientation.

Cambridge City Council has developed this guide to ensure that all employees are clear about expectations regarding internet, social media and email in order to protect them and the council from misuse of facilities and potential breach of the law.

Employees must ensure that they:

- comply with current legislation
- do not create unnecessary business risk to the council by their misuse of the internet and email
- do not bring the council into disrepute

Please ensure that you understand this guide and abide by it.

Use of email and internet are not routinely monitored but you should be aware that there may be circumstances under which monitoring of internet and email use may be carried out by the council. See section 9 for more detail.

If you are aware of, or have reasonable suspicion of, any abuses of this guidance this should be discussed with your line manager, or reported in accordance with the council's Confidential Reporting ("Whistleblowing") Policy at the earliest practicable opportunity.

For guidance on Social Media for Council business, please contact the Corporate Marketing team first to have a discussion before setting up new social media channels. Please see the link http://live.drupal.intranet.ccc.local/social-media for more information.

2. Email Guidance

You are responsible for any emails that you send so you should ensure the content is appropriate. Emails within the council's email system are copied to the 'Retain' email archiving system after 28 days and kept for 7 years using pre-set rules but remain on the email system. Emails are automatically deleted from the email system after 260 days. Your emails including private emails from a City Council email address may be subject to an access request and used as evidence in the future, for example in a court case or tribunal. Emails may be released under Freedom of Information legislation, and your mails could be quoted in the media, for instance. For more information you can view the Retain guidance on CityNet (the council's intranet site).

Guidance on handling information securely on PC's, network and mobile equipment can be found on the ICT pages of the intranet at http://live.drupal.intranet.ccc.local/content/information-security-guide

2.1 Unacceptable use of email

The following actions are examples of unacceptable behaviour:

- Sending confidential or sensitive personal data by insecure external email (see 'Security Requirements for Confidential Data' on CityNet for definitions). You can reply to emails initiated by members of the public, provided you do not include sensitive personal information in the reply.
- Sending a message, either internally or externally, which contains: illegal, offensive, obscene, or abusive material (for example, pornography); libellous, defamatory or discriminatory material; material which may bring the council into disrepute.
- Publicly voicing or associating yourself with an opinion that is in conflict with the Council's view on a matter that relates to your job. This could lead to loss of public confidence in the Council.
- Using email to bully, harass, discriminate against or victimise others.
- Disclosing your password to others.
- Using someone else's email account or network logon.
- Accessing email you are not authorised to view (i.e. you are not the recipient and do not have proxy/delegate rights or for which the proxy/delegate access you have been granted is not intended to enable you to view).
- Sending files over 20mb via email without checking with the Helpdesk.
- Emailing material that may infringe copyright/licensing laws.
- Using council email or other communication systems to set up, run or in any other way related to a personal business.
- Undertaking deliberate activities that waste staff effort or council resources, such as sending out jokes or chain letters.
- Forwarding non work related unsolicited commercial or advertising material.

Further guidance can be found on the Acceptable Use Policy for Email and Internet available on CityNet.

2.2 Remember…

- Any email you send could potentially be forwarded to others by the recipient.
- Emails are a permanent record and could appear in the public domain.
- Use the same professional language when emailing to internal and external parties that you would use for any business correspondence.
- Ensure that you arrange for emails sent to individuals or service addresses to be properly dealt with if you, someone in your team or the person who normally manages the account is out of the office.
- Email agreements can be legally binding: do not enter into contracts or place orders via e-mail without appropriate authorisation and legal advice.
- Report suspicious emails to the Helpdesk (ext. 7600).
- Send virus warnings to the Helpdesk, but not to other email users.
- Only subscribe to newsgroups and mailing lists for business purposes. Delete messages you no longer need, and only archive or save those it is important to keep.
- Use password protection on email and screensavers or lock screen.
- Automatic forwarding of email to external (i.e. non-council) accounts using rules is not permitted, as it could lead to a breach of data protection laws, with serious consequences for the council.
- Routine messages should be channelled through the Corporate Marketing team for inclusion in Insight or CityNet. Guidance can be found at http://live.drupal.intranet.ccc.local/conents/all-staff-emails. If you need to send an urgent email to the whole council you should get the permission of the Chief Executive or a Director, and indicate this in the body of the email.

3. Internet use

If you have access to the internet through your work, it is your responsibility to ensure you are aware of and follow the guidance outlined below. Please speak to your line manager if you are unsure about any aspect of your internet use.

3.1 Unacceptable use of internet

The following are examples of unacceptable use or behaviour:

- Deliberately introducing any form of computer virus or malware into the corporate network (or downloading material that you suspect may contain a virus).
- Accessing sites that contain offensive material. Systematic attempts to log on to sites containing illegal or offensive material may amount to gross misconduct and result in disciplinary action up to and including dismissal.
- Downloading software (including screen savers). If there is software on the internet that you feel you need, please contact the Helpdesk.
- Downloading copyrighted or licensed material without agreement from the copyright or licence owner.
- Using the internet to carry out any form of fraud or software, film or music piracy.
- Publishing or republishing any negative personal views and/or defamatory and/or false material about Cambridge City Council, your colleagues,

stakeholders, customers or suppliers on social networking sites, blogs or on other online sites (see section 8).
- Altering internet records or disguising user identity.
- Revealing confidential information about Cambridge City Council, its staff, suppliers or customers in a personal online posting, upload or transmission.
- Undertaking deliberate activities that waste staff effort or council resources such as downloading material with significant bandwidth e.g. MP3 or video.
- Purchasing goods for the council via the internet unless you are authorised to approve purchase orders or have an approved purchase order.
- Intruding on the privacy of members of the public by unnecessary or disproportionate searching for information about them online. This could be by pursuing them through social media or other conduct that might reasonably be perceived as prying. Even if you have a legitimate purpose (e.g. in connection with an investigation) you may need authorisation under the Regulation of Investigatory Powers Act if you are carrying out surveillance electronically. You can seek advice from the Legal Services if this authorisation is required.

3.2 Remember…

- All files should be downloaded using a device eg. laptop or PC with virus checking software installed.
- The council uses software to deny access to sites that are deemed undesirable. This does not detract from the personal duty of employees not to access illegal or offensive sites.
- In the event of any accidental blocking of legitimate sites, access will be given upon request.
- Some high level monitoring of bandwidth used and the types of site visited overall by the Council will be routinely monitored, but this will be anonymous and will not include details of who has accessed the sites.

4. Representing the Council online

In some departments, staff may be asked to represent the council online, such as on the council Facebook or Twitter pages. If you are asked to do this it is your responsibility to read and adhere to the Social Media Guidance.

You must ensure that you are authorised to disclose the information or comments you are posting and that nothing confidential is being revealed.

Remember that once you have posted something on a page it can be very difficult to remove it completely, especially if users have liked, commented or replied to it. Check the accuracy and sensitivity of what you are saying before you post it: use common sense and seek advice from your line manager or a senior colleague if unsure.

It is important that you are aware that posting and liking any content that is considered inappropriate may result in disciplinary action under the Disciplinary policy. You must be careful not to give anyone reason to doubt your political impartiality in your role as a Council Officer, including liking, sharing, favouriting or retweeting something someone else has posted that is critical or supportive of the council or an individual councillor or political group’s policies or actions.

You must ensure published content is not offensive or to the detriment of the council, and take prompt action to remove offensive comments.

5. Personal use of email and internet whilst at work

5.1 Personal use of internet

Occasional personal use of the internet is allowed, (normally this should be outside core hours). However, it should not be used for the following:

- accessing chat rooms
- operating a personal business

5.2 Personal use of email

The Council does not permit access to personal webmail accounts from corporately supplied devices. Staff must not use personal email accounts for business use. All business related email must be sent from the Council domain.

Occasional personal use of work email is permitted but:

- Emails should be short and no more than 3-4 per day
- Personal use should not detract from your work
- Email should not be used to circulate chain letters, jokes etc., that waste your time and that of other staff

5.3 Personal use of Social media

Social media sites are blocked for personal use on council computers, so you will not be able to view them at work unless you have been given access to manage a council page. If you are given access for work purposes you should not use council IT facilities to access personal social media internet pages.

If you have access to these sites on your own handheld device, occasional use is allowed; normally this should be outside of core hours.

6. Personal use of social media outside of work

Social media is the name given to a range of websites and tools that allow people to quickly and easily engage and communicate with others, such as Facebook, LinkedIn, Twitter, WhatsApp, Snapchat and Messenger. Your personal use of social media is of course your own concern, provided that it does not have an adverse effect on the council, your colleagues, our customers or suppliers.

The boundaries between professional and personal lives can become blurred when using social media: if you choose to name your employer as Cambridge City Council or are easily identified as a council employee, you should exercise great care in your posts. You must be politically neutral and unbiased in your dealings at work, whether or not you are in a ‘politically restricted’ post. This means you can’t allow your political opinions to influence or interfere with your work. If your post is politically restricted, further Political

Restriction Guidance is available on the intranet. Only senior employees or those closely involved with councillors will be "politically restricted" posts. If in doubt as to whether your post is "politically restricted" refer to your contract of employment or ask Human Resources.

It is important that any of your comments do not damage the reputation of the council. Think carefully before posting, commenting, liking, sharing or retweeting. Remember that once you have posted something on a page it can be very difficult to remove it completely, especially if users have commented or replied to it. Use common sense and if in doubt don't comment.

Bear in mind that online posts can be very quickly shared or copied by anybody they are viewed by, and seen by people you did not intend to see them. You should consider the appropriateness of revealing personal information and sharing comments with colleagues, in terms of whether this is likely to affect your reputation and professional relationships in the workplace or with external partners. Inappropriate comments made outside of work could still result in disciplinary action.

Sites such as Facebook allow you to improve your security by adjusting settings to ensure only certain information is visible to others. You should regularly check that your security settings are appropriate.

There may be occasions in the course of your work, where you have a role to play in emergency response and recovery or other high profile public events. Any emergency or similar event will result in widespread media interest and public concern. It is therefore essential that structures and processes exist to manage the demands of the media. In the circumstances, the taking of photos (and videos) in and around the incident site should only be taken with agreement from the responding emergency services as part of a response to an incident and should only be shared with the Council emergency team (Including Media team)if requested. The subsequent posting of photos or content (or links to such content) and sharing of such information will be deemed as unacceptable and insensitive behaviour which could compromise the dignity of others, impede any investigation and could bring the council into disrepute. As a consequence, any breaches will be dealt with under the Council's Disciplinary policy.

7. Safeguarding of children and adults

The council has a duty to protect the safety of children and adults at risk. If you come into contact with children and adults at risk during the course of your work, you should not make contact with them on a personal level through social media. For example, you should not 'friend' children or adults at risk that you work with on Facebook. Read the Safeguarding Policy for more information.

8. Unacceptable online behaviour

Inappropriate online behaviour, even if it takes place outside of the workplace and work time, could lead to disciplinary action at work. This action will be dealt with under the Disciplinary policy. The following are examples of unacceptable behaviour:

- Posting confidential council information online

- Posting negative, bullying or defamatory gossip or comments about councillors, colleagues, partners, stakeholders, suppliers or customers
- Criticising or arguing with colleagues, suppliers or customers
- Posting and liking inappropriate comments which might compromise dignity at work, related to a customer, supplier or colleague
- Posting photos or content (or links to such content) which could bring the council into disrepute or compromise the dignity of a colleague, partners, stakeholders, supplier or customer
- Airing grievances or posting negative comments about the council that might damage the council's reputation
- Posting content of an illegal or offensive nature that may bring the council into disrepute
- Presenting views on council matters during your personal social media use that could be misinterpreted as being the views of the council
- Posting or representing any political views if you are employed in a politically restricted post
- Posting comments or photos that compromise the protection of children and adults at risk.

If inappropriate posts on social media sites come to light, the council will consider whether to contact the host site and attempt to get the comments removed. The Council may also request that you remove such posts.

If you have concerns about an inappropriate or offensive post that has been made by a colleague, please speak to your manager or a member of Human Resources.

9. Monitoring

9.1 Monitoring of Internet use

Individual use of email and internet is not routinely monitored but the council reserves the right to monitor employees' internet use through work if there is cause for concern, such as:

- spending an excessive amount of time viewing websites that are not related to work
- a concern that online behaviour is damaging the reputation of the council or breaching confidentiality
- where specific concerns have been raised. Examples of triggers for such investigation would be management concerns (including productivity or performance issues), whistleblowing issues, complaints under the Bullying and Harassment Policy, co-operation with law enforcement agencies, as part of a disciplinary investigation, or where there has been evidence of systematic misuse. Monitoring may include the examination of records of internet sites accessed.
- Operational reasons, for example where excessive bandwidth was being used by an individual

9.2 Monitoring of emails

Emails held in individual's Email system/Outlook will not normally be opened except for operational or maintenance purposes (subject to the approval of the Head of ICT). In these cases emails and documents may be looked at unless they are marked 'personal'.

The council also reserves the right to open mail boxes and emails – even those marked personal – in connection with disciplinary, audit investigations or subject access requests. Exceptions to this are emails between employees and their representatives which should be clearly marked accordingly.

Proxy/delegate access should be used where it is important to ensure regular access to an employee's mailbox.

Full co-operation will be given if law enforcement or regulatory agencies request information about email or internet use by an employee, subject to the need for the approval of the Head of Audit or Head of Legal or Head of HR. The Head of Audit or Head of Legal or Head of HR may only give approval if satisfied that the request is for an appropriate purpose and proportionate, and that disclosure is legal. Information will not normally be disclosed other than in connection with a criminal investigation or pursuant to a court order.

Emails which are archived in Retain and Mimecast are subject to the Freedom of Information Act and Subject Access requests under the Data Protection Act. Mailboxes may therefore, in exceptional circumstances, be searched and accessed by nominated senior members of staff. There may also be circumstances where mailboxes need to be accessed for operational purposes (for instance, if a computer virus is found on the system).

10. Further information

You can get more information about acceptable behaviour at work in the Code of Conduct and on the Acceptable Use Policy for Email and Internet on CityNet the Safeguarding Policy.

If you have concerns relating to an employment related issue, you may wish to review the Bullying and Harassment policy, Grievance policy and Code of Conduct.

If you do not have access to the electronic links in the document, please contact HR.

Any comments or questions about this document should be addressed to:

Human Resources (mailto: hrbusinesspartners@cambridge.gov.uk) –to discuss inappropriate online behaviour, bullying and harassment or disciplinary matters.