HASLEMERE TOWN COUNCIL

COMPUTER, INTERNET AND EMAIL USAGE POLICY

2018

1. Introduction

1.1 Haslemere Town Council (HTC) recognises that email and internet are important information and communication systems which are used during the course of Council business and the computer network is the central hub on the Council's data storage systems. This policy provides guidelines and procedures to protect users and the Council.

1.2 This policy applies to all staff members, Councillors, IT contractors /providers and volunteers who have access to the Council's network (including Google Drive), the internet via Council computers and email facilities via both Council computers and personal devices, such as private computers, phones or tablets.

1.3 The email policy applies to any other individual who has access to a Council email address.

1.4 This policy should be read in conjunction with the Council's Data Protection Policy and Disciplinary Procedure.

1.5 All users of the Council's IT, email and internet facilities need to be aware that under the Data Protection and Freedom of Information Acts, internet and email usage reports and network documents may have to be disclosed when the Council responds to a Freedom of Information or Subject Access Request.

2. Internet usage

2.1 All users must use the internet responsibly as part of their official and professional activities.

2.2 Information obtained via the internet and published in the name of the Council must be relevant and professional. A disclaimer must be stated where personal views are expressed.

2.3 The use of the internet to access and/or distribute any kind of offensive material will not be tolerated and staff may be subject to disciplinary action. Councillors may be subject to a complaint to the Borough Council's Monitoring Officer.

2.4 The equipment, services and technology used to access the internet are the property of the Council. The Council reserves the right to monitor internet traffic and monitor and access data that is composed, sent or received through its online connections.

3. Unacceptable use of the internet

3.1 Unacceptable use of the internet by users includes, but is not limited to:

- sending or posting discriminatory, harassing or threatening messages or images
- using computers to perpetrate any form of fraud, and/or software, film or music piracy
- obtaining, using or disclosing another staff member's password without authorisation
- sharing confidential material or proprietary information outside of the Council
- hacking into unauthorised websites
- sending or posting information that is defamatory to the Council, its services, councillors and/or members of the public

- introducing malicious software onto Council computers and/or jeopardising the security of the Council's electronic communication systems
- sending or posting chain letters, solicitations or advertisements not related to Council business or activities
- passing off personal views as those representing the Council
- accessing inappropriate internet sites, web pages or chat rooms

3.2 If a staff member is unsure about what constitutes acceptable internet usage, then he/she should ask the Town Clerk for clarification.

4. Email

4.1 **Only Council email accounts must be used to conduct Council business. Personal email accounts must not be used for Council business due to potential data breaches, issues surrounding Freedom of Information or Subject Access Requests and general recommended good practice for local councils**.

4.2 Emails must not be auto-forwarded to any other account. This may result in confidential information being disclosed to unauthorised people. If needed, access can be given to email accounts for other users by the relevant Council officers with administrative powers for the Council's email accounts.

4.3 Email should be regarded as written paper documents for the purposes of production, use, retention and disclosure and can be called upon under the Freedom of Information Act 2000. Personal information should be kept in accordance with the principles established in the General Data Protection Regulations and other relevant legislation.

4.4 All Council email accounts have a private password that should be kept confidential by the user/s of that account and not shared. The Council has administrative control over email accounts and can reset passwords and give access to email accounts, where needed.

4.5 The Council reserves the right to open any email file stored on the Council's computer system or the Council's email accounts.

4.6 Care needs to be taken when registering Council email addresses on websites such as discussion forums, news groups, mailing lists, blogs etc to prevent email address being used for other purposes.

4.7 Whilst emails are generally open and transparent, some emails may not be received or read, and they may be intercepted or disclosed by other people. Users must decide whether email is the best way to exchange confidential or sensitive information.

4.8 Care must be taken when addressing emails, particularly those including sensitive, confidential or restricted information, to avoid accidentally sending them to the wrong people. Particular care must be taken when Gmail auto-completes an email address.

4.9 Email accounts must have an appropriate email signature and the relevant email disclaimer at the bottom. Such disclaimers to be provided by the Town Clerk from time to time.

4.10 All Council business emails and documents sent by users are the property of the Council and not of any individual user.

4.11 Council email address (or indeed internet or computer facilities) must not be used for:

- commercial or personal profit-making purposes or other form of financial gain (e.g. in connection with any employment other than that associated with the Council);
- activities that lead to unauthorised expenditure for the Council (e.g. excessive printing or photocopying that is not Council business);
- activities that go against Council policies or standards;
- personal interest group activity outside of a user's role;
- activities that the may cause damage, disruption, fines, penalties or negative media attention for the Council;

- excessive email conversations that may be interpreted as misuse.

4.12 The following guidelines for email use should be observed by all users of town council email addresses:

- think before you copy someone into an email conversation. Avoid replying to all unless absolutely necessary.
- use appropriate language to avoid unintentional misunderstandings
- respect the confidentiality of information contained within emails, even if encountered inadvertently
- check with the sender if there is any doubt regarding the authenticity of a message
- do not open any attachment unless certain of the authenticity of the sender
- emails which create obligations or give instructions on behalf of the Council must be sent by officers only, not councillors or other individuals
- emails must comply with common codes of courtesy, decency and privacy

5. Computer Equipment

5.1 Every user is given an individual log-on ID and password to log on to the Council's facilities, and where applicable, specific business applications, so they can access the ICT services.

5.2 Users must only use their own log-on ID and password when accessing the Council's ICT facilities; passwords must not be given to anyone else unless for operational reasons as agreed by the Town Clerk.

5.3 Users must assess any risks associated with using computer resources, removable media, internet or email to ensure it is the most appropriate tool to use.

5.4 All software used must be obtained through the Council's IT provider and have a valid licence where applicable.

5.5 In certain situations, the Council's IT provider may require access to a user's ICT equipment, with or without prior notice being given depending on the reason for access. This may be to audit, inspect, text, remove, repair or replace hardware, software or cabling, as well as for any other reasonable purpose.

5.6 Users must be vigilant when accessing the Council's network or information from public places (e.g. libraries, trains, open access computers at home etc) and/or overseas locations in order to reduce the risk of unauthorised disclosure or access.

5.7 ICT facilities, such as Office packages, internet and personal email, can be accessed for personal use providing this is done so either outside of the user's working hours or during a lunch break. Exceptions to this will need to be authorised by the Town Clerk.

5.8 Personal use must not conflict with any Council policy or the user's obligations to the Council.

5.9 Users for personal use are reminded that any documents stored on the Council's network or email accounts are accessible by the Council and if they were found to contravene Council policy or legal requirements (e.g. copyright) may be permanently removed without prior permission from the user.

5.10 Memory sticks (and other removable data storage devices) must be used with extreme care and only if the information on them is encrypted. Confidential or sensitive information must not be transferred on to any removable data storage device.

5.11 Users are expected to look after the ICT equipment, software and log-on details so that they are safe and secure at all times.

6. Computer Network

6.1 Users must be vigilant when accessing the Council's network or information from public places (e.g. libraries, trains, open access computers at home etc) and/or overseas locations in order to reduce the risk of unauthorised disclosure or access.

6.2 Users have a general and legal requirement to maintain confidentiality of information and personal data (data protection and other legislations) that they come across on the Council network.

6.3 Confidential documents such as exempt reports for Council or Committee meetings must not be shared with third parties unless authorised by the Town Clerk or Council.

6.4 Where possible, file sharing will be done on the Council's network, website or Google Drive.

6.5 Users printing documents, in particular confidential documents, from the network must accept full responsibility for keeping the document safe and secure and disposing of it appropriately.

7. Reporting and sanctions

7.1 Users must report any loss, damage, breaches, suspicious activity or anything of a worrying nature surrounding Council ICT facilities to the Town Clerk or in their absence, the Deputy Town Clerk.

7.2 Use of email which is contrary to the guidance provided in this policy may result in disciplinary action.

7.3 The Council withholds the right to remove any individual's access immediately in the event of a breach of this policy, pending an investigation.

8. Declaration

8.1 I declare that I have read, understand and agree to comply with the above Acceptable Use of Computer, Internet & Email Facilities Policy. I understand that a failure to adhere to this Policy could result in my access being withdrawn and (where relevant) disciplinary action being sought or a Member's Code of Conduct complaint being submitted.

Signed: ……

Printed: ……

Dated: ……