CULLOMPTON TOWN COUNCIL

INFORMATION AND COMMUNICATIONS TECHNOLOGY POLICY

POLICY TITLE	**Information and Communication Technology Policy**
POLICY NO	**003**
REVISION DATE	**September 2019**
REPLACES POLICY	**Email policy**
POLICY AIM	**The Council recognises that email and internet are important information and communication systems which are used during the course of Council business. This policy provides guidelines and procedures to protect both users and the Council and it should be read in conjunction with the Council's Information and Information Security Policy and Disciplinary Procedure.**

1. INTRODUCTION

1.1. This email and computer network policy applies to all Council staff and councillors in their access to the Council's computer network and Council email addresses via both Council computers and personal devices, such as private computers, mobile phones or tablets.

1.2. Under the GDPR (2018) 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.

1.3. Access to Council email, internet or ICT facilities will not be provided until this policy has been read and signed by the user, declaring an understanding of all the points within.

1.4. Hall users will be issued with a different password from that used by Council staff.

2. IT EQUIPMENT USE

2.1 It is very important that the Council is able to keep its data secure. To assist with this, all employees are required to comply with instructions that may be issued from time to time regarding the use of Council-owned computers or systems.

2.2 Use of Council ICT devices must be kept secure and password protected at all times.

2.3 Your passwords are important pieces of confidential information and should be treated that way. Do not share passwords with others, and make sure that they are not written down anywhere where an unauthorised person can find it.

2.4 Unauthorised access to or use of any of the Council's systems will amount to gross misconduct.

3. EMAIL

3.1 Use of email is encouraged as it provides an efficient and cost-effective system of communication and all Councillors will be provided with a Town Council email address.

3.2 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.

3.3 All Council email accounts should 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 if necessary e.g. in the case of a forgotten password, can reset passwords and give access to email accounts, where needed. Any access will be carried out by the designated Officer who has administrative control.

3.4 The Council reserves the right to open any file stored on the Council's computer system or the Council's email accounts. In the case of emails, such access will only be carried out in the event of the death, long term incapacitation, resignation or deselection of an elected or co-opted member or in the event of the death, long term incapacitation, resignation or other circumstance in the case of officers and members of staff. Access may be given to the Police in the event of a criminal investigation. Any access will be carried out by the designated Officer who has administrative control.

3.5 It is recommended that only Council email accounts should be used to conduct Council business. Personal email accounts should 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. Confidential information transmitted from the council offices by the officers and staff of the council will only be transmitted to the officially supplied cullomptontowncouncil.gov.uk email address issued to elected and co-opted members.

3.6 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 addresses being misused.

3.7 External networks such as the internet, are not guaranteed to be secure and confidentiality cannot be assured when using these networks. 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.

3.8 All Councillors will be provided with a cullomptontowncouncil.gov.uk email address and it is strongly recommended that when corresponding in their role as a Town Councillor and for all Council business that this email address is used. This will help to ensure that all Council related information, in particular, confidential and sensitive data, is properly protected.

3.9 Once a Councillor dies, suffers from long term incapacitation, resigns or is deselected, his/her email address and all its contents will be deleted with email correspondence being retained in archive in accordance with the Council's document retention policy.

3.10 To avoid accidentally sending messages to an unintended recipient, care must be taken when addressing emails, particularly those including sensitive, confidential or restricted information. Particular attention must be paid when using the 'Reply All' & 'Forward' buttons.

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

3.12 Do not forward on emails or email threads as they may contain personal data. Copy and paste information from an email if you want to pass it on, rather than forwarding on an email to remove the originator's email address from the header.

3.13 Council email addresses must not be used for:

3.13.1. any political activities (Officers & Staff only) .
3.13.2. 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).
3.13.3. activities that lead to unauthorised expenditure for the Council.
3.13.4. (e.g. excessive printing or photocopying that is not Council business).
3.13.5. activities that go against Council policies or standards.
3.13.6. personal interest group activity outside of a user's role.
3.13.7. activities that may cause damage, disruption, fines, penalties or negative media attention for the Council.
3.13.8. excessive email conversations that may be interpreted as misuse.

3.14 The following guidelines for email use should be observed by all staff members and councillors:

3.14.1. use appropriate language to avoid unintentional misunderstandings.

3.14.2. respect the confidentiality of information contained within emails, even if encountered inadvertently.
3.14.3. check with the sender if there is any doubt regarding the authenticity of a message.
3.14.4. do not open any attachment unless certain of the authenticity of the sender.
3.14.5. only copy emails to others where appropriate and necessary.
3.14.6. emails which create obligations or give instructions on behalf of the Council must be sent by officers only, not councillors or other individuals.
3.14.7. emails must comply with common codes of courtesy, decency and privacy.
3.14.8. All email correspondence should be dealt with in a professional and diligent manner.

3.15 Using a Council email address to send inappropriate material, including content of a sexual or racist nature, is strictly prohibited and may amount to gross misconduct for Council staff and Councillors being referred to the Mid-Devon District Council's Monitoring Officer. Should any offensive or inappropriate content be received via email, the Town Clerk should be informed at earliest opportunity so that appropriate action can be taken.

4. INTERNET USE

4.1 Staff Members of the Council and Councillors and are encouraged to use the internet responsibly as part of their official and professional activities.

4.2 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.*

4.3 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 Mid-Devon District Council's Monitoring Officer.

4.4 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.

4.5 Unacceptable use of the internet by staff members includes, but is not limited to:

4.5.1. sending or posting discriminatory, harassing or threatening messages or images.
4.5.2. using computers to perpetrate any form of fraud, and/or software, film or music piracy.
4.5.3. obtaining, using or disclosing another staff member's password without authorisation.

4.5.4. sharing confidential material or proprietary information outside of the Council.
4.5.5. hacking into unauthorised websites.
4.5.6. sending or posting information that is defamatory to the Council, its services, councillors and/or members of the public.
4.5.7. introducing malicious software onto Council computers and/or jeopardising the security of the Council's electronic communication systems.
4.5.8. sending or posting chain letters, solicitations or advertisements not related to Council business or activities.
4.5.9. passing off personal views as those representing the Council.
4.5.10. accessing inappropriate internet sites, web pages or chat rooms.

4.6 If a staff member is unsure about what constitutes acceptable internet usage, then the appropriate Line Manager should be contacted in the first instance for guidance.

4.7 Employees and Councillors with access to the internet on Council-owned devices should use that access responsibly. Excessive personal use during working hours will be treated as misconduct. From time to time the Council may block access to sites which it considers inappropriate but whether or not a specific site has been blocked, employees must not use the internet to view or download offensive or sexually explicit material. Any attempt to do so may, depending on the circumstances, amount to gross misconduct leading to dismissal.

4.8 Employees must not download any software, plug-ins or extensions on to Council-owned devices unless this is first cleared by the Town Clerk nor must employees use Council-owned devices to download music, video or any other entertainment content.

4.9 Firewalls and anti-virus software may be used to protect the Council's systems. These must not be disabled or switched off without the express authorisation of the Town Clerk.

5. SOCIAL MEDIA

5.1. An employee's behaviour on any social networking or other internet site must be consistent with the behaviour required of employees generally. Where it is possible for users of a social media site to ascertain who you work for, then you should take particular care not to behave in a way which reflects badly on the Council. Inappropriate or disparaging comments about the Council, colleagues or the town will be treated as misconduct. Because social media interactions can be copied and widely disseminated in a way that you may not be able to control, the Council will take a particularly serious view of any misconduct that occurs through the use of social media.

5.2. You must not operate a social media account or profile that purports to be operated on or on behalf of the Council without express permission to do so from

your manager. Councillors should ensure that all social media accounts make it clear that the views expressed are their own and do not necessarily reflect the official view of the Council.

6. REPORTING AND SANCTIONS

6.1. 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 duty manager in the Council offices.

6.2. If a councillor receives an email from a staff member which they believe is contrary to the guidance provided in this policy, it should be reported to the Clerk who will investigate the matter and may consider use of the Council's formal disciplinary procedure depending on the severity of the event.

6.3. If a staff member receives an email from another staff member which they believe is contrary to the guidance provided in this policy, it should be reported to the Clerk who will investigate the matter and may consider use of the Council's formal disciplinary procedure depending on the severity of the event.

6.4. If a staff member receives an email from a councillor which they believe is contrary to the guidance provided in this policy, the staff member may look to raise things informally with the Town Clerk (or in the case of the Town Clerk, the Mayor) in the first instance but is entitled to consider use of the Council's Grievance Policy and/or report the issue through the procedures outlined in the Member's Code of Conduct.

6.5. If a staff member or councillor believes that there has been inappropriate use of any of the Council's ICT facilities (whether it be email, internet or computer network) this should be reported to the Town Clerk to investigate. In the case of the Town Clerk wishing to report a suspected breach of this policy or being the staff member in question of a suspected breach, the Mayor should be informed in the first instance, who will work in consultation with the Chair of the Policy, Finance & Personnel Committee to investigate any claim.

6.6. The Council reserves the right to remove a staff member's access immediately in the event of a breach of this policy, pending an investigation.

7. DECLARATION

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: …….

In my capacity of (e.g.Councillor)…….

Name (Printed): ……

Dated: ……..