BRANDON & BYSHOTTLES PARISH COUNCIL

Acceptable Use of Computer, Internet & Email Facilities Policy

1. Introduction

The Council 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 to the Council's data storage systems. This policy provides guidelines and procedures to protect users and the Council.

This policy applies to all staff members who have access to the Council's network, the internet via Council computers and email facilities via both Council computers and personal devices, such as private computers, phones or tablets.

The email policy and computer network policy applies to all councillors in their access to the Council's computer network and Council email addresses.

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

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

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; all users of Council ICT facilities must be aware of this.

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.

2. Internet usage

Staff members are encouraged to use the internet responsibly as part of their official and professional activities.

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.

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 Durham County Council's Monitoring Officer.

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

Unacceptable use of the internet by staff and members 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

If a staff or member is unsure about what constitutes acceptable internet usage, then he/she should ask his/her line manager or The Clerk for further guidance and clarification

4. Email

Use of email is encouraged as it provides an efficient system of communication.

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.

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.

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

Only Council email accounts must 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.

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.

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.

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 Outlook auto-completes an email address.

Emails should not be auto-forwarded to any other account as 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.

Email accounts must have an appropriate email signature and the relevant email disclaimer at the bottom of all emails written.

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

Email distribution lists should not be created on individual email accounts; this is to ensure contact details are not out of date, prevent accidental sharing of contact details and to comply with data protection legislation. Data subjects have a right to 'be forgotten'; email addresses stored on individual email accounts will easily allow contact details to be inadvertently stored.

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

- any political activities;
- 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.

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

- 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
- only copy emails to others where appropriate and necessary
- 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

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.

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 at all.

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.

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

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.

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.

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 user's line manager.

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

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.

Memory sticks (and other removable data storage devices) must be used with extreme care to stop Council information being lost or disclosed. Confidential or sensitive information must not be transferred on to any removable data storage device.

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

Users accessing the network from Council offices will have automatic access once they have logged in to the Council facilities as per section 5 above.

Users must only use their own log-on ID and password when accessing systems; log-on ID and passwords must not be given to anyone else at all and must be stored securely.

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.

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.

Documents from the Council network must not be shared with third parties unless an authorised instruction from a Council officer is given; councillors or staff members may not take it upon themselves to share information held by the Council without prior authorisation.

Councillors are given access to a specific information. Council officers will refrain from emailing documents, in particular those of sensitive or confidential nature, and instead will upload these documents to the network drive and inform Councillors that this is ready to be viewed.

The above includes exempt reports for Council or Committee meetings.

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.

Recommended disposal of Council documents, particularly confidential, is via the shredder in the Council offices.

7. Reporting and sanctions

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

Advice on computer, email or network related issues should in the first instance be sought from the Clerk or in their absence, the Assistant Clerk or failing that, may be sought from the Council's IT Support. Councillors should note that advice can only be given on Council facilities i.e. we cannot provide advice on problems with a personally-owned computer but can provide support with network access or Council email issues.

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.

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.

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 their line manager 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.

If a staff member or councillors 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 Clerk to investigate.

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

In the case of the Clerk wishing to report a suspected breach of this policy or being the staff member in question of a suspected breach, the Chairman should be informed in the first instance, who will work in consultation with the Chairman of Personnel to investigate any claim.

8. 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: …….

Printed: ……

Dated: ……..