ST CLEER
COMMUNICATIONS AND IT POLICY

1. Parish Council Correspondence

1.1 The point of contact for the council is the Parish Clerk, and it is to the Parish Clerk that all correspondence for the Parish council should be addressed.

1.2 The Parish Clerk should deal with all correspondence following a meeting.

1.3 No individual Councillor or Officer should be the sole custodian of any correspondence or information in the name of the Parish council, a committee, sub-committee or working party. In particular, Councillors and Officers do not have a right to obtain confidential information/documentation unless they can demonstrate a 'need to know'.

1.4 All official correspondence should be sent by the Parish Clerk in the name of the council using council letter headed paper.

1.5 Where correspondence from the Parish Clerk to a Councillor is copied to another person, the addressee should be made aware that a copy is being forwarded to that other person (e.g. copy to xx).

B. Agenda Items for Council, Committees, Sub-Committees and Working Parties

(i) The agenda should be clear and concise. It should contain sufficient information to enable Councillors to make an informed decision, and for the public to understand what matters are being considered and what decisions are to be taken at a meeting.

(ii) Items for information should be kept to a minimum on an agenda.

(iii) Where the Parish Clerk or a Councillor wishes fellow Councillors to receive matters for "information only", this information will be circulated via the Parish Clerk.

C. Communications with the Press and Public

(i) The Parish Clerk will clear all press reports, or comments to the media, with the Parish Chair or the Chair of the relevant committee as appropriate.

(i) Press reports from the council, its committees or working parties should be from the Parish Clerk or an officer or via the reporter's own attendance at a meeting.

(ii) Unless a Councillor has been authorised by the council to speak to the media on a particular issue, Councillors who are asked for comment by the press should make it clear that it is a personal view and ask that it be clearly reported as their personal view.

(iii) Unless a Councillor is absolutely certain that he/she is reporting the view of the council, they must make it clear to members of the public that they are expressing a personal view.
(iv) If Councillors receive a complaint from a member of the public, this should be dealt with under the Council's adopted complaints procedure, or via a council agenda item.

D. Councillor Correspondence to external parties
(i) Individual councillors are responsible for their own correspondence. The Parish Council does not provide a secretariat for such purpose. Councillors must ensure they make clear where they are informing on official policy and where they are stating their personal views.
(ii) A copy of all outgoing correspondence relating to the council or a Councillor's role within it, should be sent to the Clerk, and it be noted on the correspondence, e.g. "copy to the Clerk" so that the recipient is aware that the Clerk has been advised.

E. Communications with Parish Council Staff
(i) Councillors must not give instructions to any member of staff, unless authorised to do so (for example, three or more Councillors sitting as a committee or sub-committee with appropriate delegated powers from the council).
(ii) No individual Councillor, regardless of whether or not they are the Chair or the Chair of a committee or other meeting, may give instructions to the Clerk or to another employee which are inconsistent or conflict with council decisions or arrangements for delegated power.
(iii) Telephone calls should be appropriate to the work of the Parish council.
(iv) Instant replies should not be expected to e-mails from the Clerk; reasons for urgency should be stated;
(v) Councillors should acknowledge their e-mails when requested to do so.
(vi) For meetings with the Clerk or other officers an appointment should be made wherever possible, meetings should be relevant to the work of that particular officer and councillors should be clear that the matter is legitimate council business and not matters driven by personal or political agendas.

2.8 **Computer use**

ST CLEER
COMMUNICATIONS AND IT POLICY

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.
Council portable IT devices must be kept secure and password protected at all times.
Your computer password is an important piece of confidential information and you should treat it that way. Do not share it with others, and make sure that it is not written down anywhere where an unauthorised person can find it.
Unauthorised access to any of the Council's systems will amount to gross misconduct.

Email

All email correspondence should be dealt with in the same professional and diligent manner as any other form of correspondence.

If you have a Council email account you should be mindful of the fact that any email that you send will be identifiable as coming from the Council. You should therefore take care not to send anything via email that may reflect badly on the Council. In particular, you must not send content of a sexual or racist nature, junk mail, chain letters, cartoons or jokes from your Council email address.

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/breach of the Code of Conduct. Should you receive any offensive or inappropriate content via email you should inform the Parish Clerk of this as soon as possible so that they can ensure that it is removed from the system.

You should also take care that emails will be seen only by the person intended. Particular care should be taken when sending confidential information that the email has been correctly addressed, marked 'private' and not copied in to those not authorised to see the information. Sending confidential information via email without proper authorisation or without taking sufficient care to ensure that it is properly protected will be treated as misconduct.

While a reasonable amount of personal use of email is perfectly acceptable, your email remains the property of the Council and you should not use your Council email to send or receive any information that you regard as private. The Council may, in the course of its operation, read emails that you have sent or received - although in the absence of evidence of wrongdoing the Council will try to avoid reading personal emails if possible.

Internet use
Employees 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.

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

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 Parish Clerk.

Social media
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 Parish 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.

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.

ST CLEER
COMMUNICATIONS AND IT POLICY

Acceptable Use of Computer, Internet & Email Facilities Policy

1. Introduction

1.1 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 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 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.

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

~~1.4~~ The email policy applies to any other individual who has access to a Council email address~~, such as but not limited to, the Young Chair and Deputy Young Chair.~~

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

1.6 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.

1.7 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

2.1 Staff members are encouraged to 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 Lewes District 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 staff 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

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

4. Email

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

4.2 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.

4.3 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.

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

4.5 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.

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 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.

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 Outlook auto-completes an email address.

4.9 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.

4.10 Email accounts must have an appropriate email signature and the relevant email disclaimer at the bottom of all emails written. Such disclaimers to be provided by the Clerk

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

4.12 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. Email distribution lists should be stored on the Council's Excel Address Book.

4.13 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 may cause damage, disruption, fines, penalties or negative media attention for the Council;
- excessive email conversations that may be interpreted as misuse.

4.14 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

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 at all.

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 user's line manager.~~

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 to stop Council information being lost or disclosed. 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 accessing the network from Council offices will have automatic access once they have logged in to the Council facilities as per section 5 above.~~

~~6.2 Those accessing the network remotely, such as councillors and staff at remote locations or home working, will be given an individual log-on ID and password to log on to the Council's network through SIRAS.~~

~~6.3 Users must only use their own log-on ID and password when accessing SIRAS; log-on ID and passwords must not be given to anyone else at all and must be stored securely.~~

~~6.4 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.~~

6.5 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.

~~6.6 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.~~

~~6.7 Councillors are given access to a specific network drive of the Council's. 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.~~

6.8 The above includes exempt reports for Council or Committee meetings; these reports will be provided through the network only, not by email or in hard copy.

6.9 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.

6.10 Recommended disposal of Council documents, whether confidential or not, is via the waste paper and confidential waste paper bins in the Council offices. If unsure about which to use, please seek the advice of a Council officer.

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 Parish Clerk or in their absence, the ~~duty manager in the Council offices.~~ chair

~~7.2 Advice on computer, email or network related issues should in the first instance be sought from a staff member or failing that, may be sought from the Council's IT Support (Schools ICT on 01273 482 519). Councillors should note that advice can only be given on Council facilities i.e. Schools ICT cannot provide advice on problems with a personally-owned computer but can provide support with network access or Council email issues.~~

7.3 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.

7.4 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.

7.5 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.

7.6 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 Parish Clerk to investigate.

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

7.8 In the case of the Parish Clerk wishing to report a suspected breach of this policy or being the staff member in question of a suspected breach, the Chair should be informed in the first instance, who will work in consultation with the Chair 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: …………………………………………………………………