CHALFONT St. PETER PARISH COUNCIL

Council Office, adj. The Community Centre, Gravel Hill, Chalfont St Peter, Bucks, SL9 9QX
Tel & Fax: 01753 891582 email: clerk@chalfontstpeter-pc.gov.uk
Website: www.chalfontstpeter-pc.gov.uk

Clerk: Mrs Debbie Evans Deputy Clerk: Nick Stayt

ELECTRONIC INFO & COMMS SYSTEM POLICY

(Taken from the Staff Handbook – July 2011)

30.1 All staff are expected to protect our electronic communications systems and equipment from unauthorised access and harm at all times. Failure to do so may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

Equipment security and passwords

30.2 Staff are responsible for the security of the equipment allocated to or used by them, and must not allow it to be used by anyone other than as permitted by this handbook.

30.3 If given access to the e-mail system or to the internet, staff are responsible for the security of their terminals. If leaving a terminal unattended or on leaving the office they should ensure that they lock their terminal or log off to prevent unauthorised users accessing the system in their absence. Staff without authorisation should only be allowed to use terminals under supervision.

30.4 Passwords must be kept confidential and must not be made available to anyone else unless authorised by the Clerk.

Systems and data security

30.5 Staff should not delete, destroy or modify existing systems, programs, information or data which could have the effect of harming our business or exposing it to risk.

30.6 Staff should not download or install software from external sources without authorisation from the Clerk. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Incoming files and data should always be virus-checked.

30.7 No device or equipment should be attached to our systems without the prior approval of the Clerk. This includes any USB flash drive, MP3 or similar device, PDA or telephone. It also includes use of the USB port, infra-red connection port or any other port.

30.8 Workers should exercise caution when opening e-mails from unknown external sources or where, for any reason, an e-mail appears suspicious (for example, if its name ends in .ex). The Clerk should be informed immediately if a suspected virus is received. We reserve the right to block access to attachments to e-mails for the

purpose of effective use of the system and for compliance with this part of our handbook. We also reserve the right not to transmit any e-mail message.

30.9 Staff should not attempt to gain access to restricted areas of the network, or to any password-protected information, unless specifically authorised.

30.10 Staff using laptops or wi-fi enabled equipment must be particularly vigilant about its use outside the office.

E-mail etiquette and content

30.11 E-mail is a vital business tool, but an informal means of communication, and should be used with great care and discipline. Staff should always consider if e-mail is the appropriate means for a particular communication and correspondence sent by e-mail should be written as professionally as a letter or fax. Messages should be concise and directed only to relevant individuals. Our standard disclaimer should always be included.

30.12 Staff should not send abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory e-mails. Anyone who feels that they have been harassed or bullied, or are offended by material received from a colleague via e-mail should inform[their line manager.

30.13 Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Staff should assume that e-mail messages may be read by others and not include anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain.

30.14 E-mail messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an e-mail cannot be recovered for the purposes of disclosure. All e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software.

30.15 In general, staff should not:

(a) send or forward private e-mails at work which they would not want a third party to read;

(b) send or forward chain mail, junk mail, cartoons, jokes or gossip;

(c) contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them;

(d) agree to terms, enter into contractual commitments or make representations by e-mail unless appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written at the end of a letter;

(e) download or e-mail text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;

(f) send messages from another worker's computer or under an assumed name unless specifically authorised; or

(g) send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure.

Use of the internet

30.16 When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is of a kind described in paragraph 33.31, such a marker could be a source of embarrassment to the visitor and us, especially if inappropriate material has been accessed, downloaded, stored or forwarded from the website. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature.

30.17 Staff should therefore not access any web page or any files (whether documents, images or other) downloaded from the internet which could, in any way, be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK, it may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of our Electronic Information and Communications Systems Policy.

Personal use of systems

30.18 We permit the incidental use of internet, e-mail and telephone systems to send personal e-mail, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must be neither abused nor overused and we reserve the right to withdraw our permission at any time.

30.19 The following conditions must be met for personal usage to continue:

(a) use must be minimal and take place substantially out of normal working hours.
(b) use must not interfere with business or office commitments;
(c) use must not commit us to any marginal costs; and
(d) use must comply with the policies set out in this handbook including the Equal Opportunities Policy, Anti-harassment Policy, Data Protection Policy and Disciplinary Procedure.

Monitoring of use of systems

30.20 We reserve the right to retrieve the contents of messages or check searches which have been made on the internet for the following purposes (this list is not exhaustive):
(a) to monitor whether the use of the e-mail system or the internet is legitimate;
(b) to find lost messages or to retrieve messages lost due to computer failure;
(c) to assist in the investigation of wrongful acts; or
(d) to comply with any legal obligation.

Inappropriate use of equipment and systems

30.21 Access is granted to the internet, telephones and other electronic systems for legitimate business purposes only. Incidental personal use is permissible provided it is in full compliance with our rules, policies and procedures (including this policy, the Equal Opportunities Policy, Anti-harassment Policy, Data Protection Policy and Disciplinary Procedure).

30.22 Misuse or excessive use or abuse of our telephone or e-mail system, or inappropriate use of the internet in breach of this policy will be dealt with under our Disciplinary Procedure. Misuse of the internet can, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by participating in online gambling or chain letters or by creating, viewing, accessing, transmitting or downloading any of the following material will amount to gross misconduct (this list is not exhaustive):

(a) pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);
(b) offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients;
(c) a false and defamatory statement about any person or organisation;
(d) material which is discriminatory, offensive, derogatory or may cause embarrassment to others;
(e) confidential information about us or any of our staff or clients (which you do not have authority to access);
(f) any other statement which is likely to create any liability (whether criminal or civil, and whether for you or us); or
(g) material in breach of copyright.

Any such action will be treated very seriously and is likely to result in summary dismissal.

30.23 Where evidence of misuse is found we may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in our Disciplinary Procedure. If necessary such information may be handed to the police in connection with a criminal investigation.