Appendix B

Central Bedfordshire Council

# ICT Acceptable Use Policy

Version 0.4

March 2009

**Not Protected**

## Policy Governance

| | |
|---|---|
| Accountable Director | Director of Corporate Resources |
| Policy Author (Title) | Assistant Director (ICT) |
| Approved By (Title) | |
| Date Approved | |
| Issue Date | |
| Review Date | |
| Person Responsible for Review (Title) | |
| Include in Publication Scheme (Y/N) | |
| Publish to Web (Y/N) | |
| Intranet Link | |
| Circulation | This policy is to be made available to and observed by all Central Bedfordshire Council officers, both social care and otherwise.<br>There will be an ongoing professional development and educational strategy to accompany the implementation of this policy. |
| Implementation Plan in place (Y/N) | |

## Policy Approval

Central Bedfordshire Council acknowledges that information is a valuable asset, it is therefore wholly in its interest to ensure that the information it holds, in whatever form, is appropriately governed, in terms of protecting the interests of all of its stakeholders.

This policy and its supporting standards and work instructions are fully endorsed by the Corporate Management Team through the production of these documents and their minuted approval.

I trust that all officers, contractors and other relevant parties will, therefore, ensure that these are observed in order that we may contribute to the achievement of the Council's objectives and the delivery of effective services to our community.

**Chief Executive:** ______________________________

**Date** ______________________________

The current version of the Central Bedfordshire Council's ICT Acceptable Use Policy is available from the website at www.centralbedfordshire.gov.uk.

Alternatively, a copy can be obtained by writing to the Information Governance Manager at:

Central Bedfordshire Council
Priory House
Chicksands
Shefford
SG17 5TQ

## Revision History

| Version Number | Revision Date | Summary of Changes | Author |
|---|---|---|---|
| 0.1 | December 2008 | First collation | Simon Woods |
| 0.2 | 27th Feb 2009 | Update | Simon Woods |
| 0.3 | 9th March 2009 | Update | Robert Wood |
| 0.4 | 12th March 2009 | Update | Robert Wood |

## PURPOSE & SCOPE

The digital age brings with it many advantages as well as many threats. If used correctly, computer and telephony services can provide local authorities with the ability to serve our citizens, customers & partners efficiently in an economical, secure, accessible and legally compliant manner. However, to meet this goal and to get the most out of such systems, they need to be used in a co-ordinated and structured way, with users following defined policies and guidance. This policy sets out the mandatory measures & requirements, as well as some best practice advice applicable to the use of the Council's Information & Communication Technology (ICT) systems. It should be read in conjunction with the following council policies & procedures in particular:

- Data Protection Policy (DP)
- Freedom of Information Policy (FOI)
- Information & Records Management Policy
- Information Governance and Security Policy
- ICT procedures available on the Intranet
- Any applicable system specific or local service management guidance

This policy applies to all established employees, temporary employees, agency staff and consultants/contractors who are provided with access to any council provided ICT service not designated as a public facility. For the purpose of this policy these people will be termed "users". Managers are responsible for ensuring all users under their control (be that employees or temporary/contract staff) are aware of, understand and adhere to this policy in all respects. Failure to adhere to the mandatory measures & requirements in this policy will be treated as a serious case of misconduct and is liable to result in a final written warning or even immediate dismissal as per the council disciplinary procedure. Continued and repeated failure to adhere to significant items of best practice may also be considered as a lack of capability or misconduct.

The Council provides ICT systems to its users for business use only (including recognised personal development in the case of employees). Personal use of such systems is generally forbidden (although limited personal use is allowed in certain instances as defined by this document). For the purposes of clarification, limited personal use (where permitted) never allows personal business use or other private use for financial gain. The reason for this policy is that all ICT usage has an indirect cost (be that storage space for files & E-Mails, network capacity for browsing the internet or call charges for telephones), and it is not appropriate for these services to be funded from public money when for personal use. Although perhaps minor when considered on a per person basis, personal use when accumulated over the whole organisation can be very significant in terms of the resources it uses and therefore the cost it attracts. Personal use of certain items (e.g. council provided mobile phones) can also give rise to tax implications for the individual and this complicates the tax (and therefore administration) affairs of both the organisation and individual.

All access to council ICT systems is therefore based upon business necessity and related to the post held and role undertaken. It is the responsibility of both the individual and the line manager (where appropriate) to ensure that the user is adequately trained to use the ICT services provided in an efficient and acceptable manner. Please remember that a programme of free ICT training is available and it is the expectation of the organisation that users will proactively seek to avail themselves of any training that they might need and that managers will support this. Managers are expected to satisfy themselves as to the suitability of candidates ICT skills during the recruitment process and ensure ICT training and skills needs analysis is an integral part of annual appraisals for new and established employees alike.

Whilst being mindful of the general right of employees to privacy at work, in order to ensure the effective operation of this policy and to safeguard the organisation’s greater interests, the Council reserves the right to use automated tools and selected manual intervention, where appropriate and necessary, to monitor usage of business ICT systems and services (In particular the Internet and E-Mail) in accordance with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

## TELEPHONY

The Council may provide users with a variety of telephony services including desktop phones, mobiles and answer phone services. Providing the nature, frequency, call length or other aspects do not reach an unacceptable level that affect your performance of your role or that of your colleagues, council phones may be utilised for **incoming** personal call use.

Generally council provided phones (fixed or mobile) may only be utilised for outgoing personal use, where it is an emergency or another very occasional and urgent genuine requirement exists (for example calling your partner to tell them that you will have to work late unexpectedly).

The ability for users to make personal calls and then reimburse the Council for the subsequent cost is not available. However for users with corporate Orange mobile phones (but not PDA's), it is possible to have a second personal line added to your phone that will be billed individually to your home address. If you are interested in such a facility, please contact the ICT ServiceDesk.

People may use their own personal (non council provided) mobile phones in the office at any time, providing the nature, frequency, call length or other aspects do not reach an unacceptable level that affect your performance of your role or that of your colleagues,

For users with council mobile phones, the following best practice guidelines should be followed:

- Store all mobile numbers in "SIM" Card memory rather than phone memory
- Ensure that a "SIM" pin is entered and enabled and that no phone pin is used
- Ensure that your line manager is provided with your SIM pin (especially before leaving the organisation)
- Avoid overt use of your phone in public places to minimise theft and personal safety issues
- Never use a council provided phone whilst driving (even hands free)
- Ensure in all meetings that your phone/PDA is switched off or if required for an expected urgent call that the device is switched to silent and the meeting participants informed at the beginning of the meeting that you might need to leave the room to take an urgent call.
- Ensure in all meetings that you do not use any PDA device unless actively required as part of the meeting you are attending.
- Failure to follow these latter guidelines is often disruptive and fails to show respect to your colleagues.

Where individuals are provided with an answerphone service (either via a council provided mobile phone or via their desktop phone), the following best practice guidelines should be followed:

The answerphone is provided for situations when you are not available or genuine circumstances when you need to remain undisturbed (e.g. a meeting or staff appraisal). Specifically it must not be used to “screen” incoming calls or to avoid answering calls unless there is a genuine need as described above. For the sake of clarity, “being busy” or “needing to concentrate” is not usually an acceptable reason for using voicemail when you are otherwise available. This is important in providing good customer service for both internal and external facing roles alike.

You should ensure that your outgoing message is changed regularly (ideally on a daily basis). You should strongly consider giving the following information in your message:

- Today’s date
- An expectation of when you will next be in the office and/or available
- An alternative contact for urgent queries

This information will allow callers to decide upon the most appropriate action upon hearing your message. You should check for messages left and respond as appropriate on a regular basis and always as one of your first activities upon returning to the office or becoming available again.

All users are provided with an internal telephone directory and are expected to ensure that their own entry is kept accurate with respect to telephony details as well as job title, location etc. Repeated failure to do this will be considered a serious matter as it impacts upon colleagues across the authority and their ability to contact you, especially for Customer Services.

Finally, when using voice communications, be aware of divulging sensitive or confidential information of a business or personal nature, unless you are sure of the other person’s identity (Fraudsters often claim to be from an official institution) and are confident you cannot be overheard.

## SECURITY OF SYSTEMS AND INFORMATION

### Sharing of Logon Passwords Prohibited

It is the responsibility of each user to maintain the confidentiality of her/his personal passwords. The sharing of such passwords with another person is strictly forbidden and represents gross misconduct in **ALL** circumstances. Passwords should not be written down. (The only exceptions to this are "Pins" and "File" passwords that cannot be changed in emergencies by the ICT service. In this scenario, any emergency record of the password should be placed in a closed envelope signed across the seal, then stored in a secure location). Users must not attempt to access a computer system where they do not have a user account, nor should a user log on to any system and let someone else use the computer whilst logged on under their name. If you have requirements to share data (either regularly or in someone's absence), then providing advice is sought from ICT in advance, there is **never** a need or excuse to share a personal password.

In certain occasional and emergency circumstances, access to an individual's account may be granted to their line manager, Internal Audit or other appropriate party (via password reset or other methods). However the following should be noted:

- This process will require the written authorisation of a Director giving a clear business justification for doing so.
- This process will not be enacted for an event that could reasonably be foreseen in advance (e.g. Staff Holiday).
- The party gaining access to the account must abide by all relevant legislation, policies and guidance and only use the access for the specific justification given.

It is accepted that certain individuals will need to share "system" logins (for example administrator passwords) and record them in a secure centralised place. This is permissible under the policy, but must be reflected as a specific exemption on the permissions form signed by the user. However all other aspects of the policy still apply for example not leaving screens unattended or writing passwords down in an inappropriate way.

### Secretarial/PA Facility

Managers wishing to allow their Secretary or PA to access all non-confidential e-mail messages may arrange for this facility to be made available by setting up the appropriate protocol within the e-mail system. However, managers must not divulge to their secretary or PA their personal passwords.

## Password Security

Personal passwords should be changed at least every 30 days whether users are prompted by the system or not to change their computer password. Passwords must be a mixture of upper and lower case numbers, include numbers and must be a minimum of 8 characters in length, and should not be obvious (e.g. names of relatives or pets), which would make it easier for others to logon using that password and user identity. Please remember that a computer can only identify an individual by their username and password. As the username is usually known or easily discoverable, the password is critical in identifying you to the system and therefore your permissions and usage and restricting unwanted access. You are therefore expected to take all reasonable steps to ensure your password remains confidential to you.

## Positioning of Computer Screens

Computer screens should be positioned on desks in such a way so as to minimise the opportunity for data displayed on the screen to be viewed by unauthorised persons such as those walking past desks or visiting the office. This is particularly important in areas the public are present or where information classed as “Protected” or “Restricted” is being dealt with. However such considerations should never override health and safety aspects. If users have any concerns regarding the ergonomics of their working position, they must notify their line manager in writing immediately.

## Absence from Workstations

All users must use ‘Ctl-Alt-Delete’ to lock their screen when they are out of view of their workstation. When they leave their workstation for 60 minutes or more, users should log-out of the applications they are using and the machine, by selecting the ‘Log Out’ option after pressing ‘Ctl-Alt-Delete’. This will help ensure that data is protected in the event of a system crash and recovery procedures are made more efficient. At the end of the day users must choose the ‘Shut Down’ option and power off their machine (if not automatic). This requirement is critical for reasons of system backup and environmental considerations. (Ensure screens are switched off an not just on standby).

## Cancellation of Logon ID with Termination of Employment

The logon ID (username) of an employee who is leaving is to be cancelled as of the date and time specified by the employee's line manager. It is the manager’s responsibility to inform the ICT servicedesk to cancel the logon ID, even though the process might be initiated by the HR service. The line manager is responsible for arranging the appropriate handling of ex-employees communications, be that telephony or E-Mail. With the increasing availability of remote access tools, this step is critically important as a valid logon ID in the possession of a user who has left will still potentially grant access to council systems, data and information.

## Data Security & Information Management

All files should be stored within the EDRMS (electronic and document records management systems or on network drives as such data is held securely and is backed up to mitigate against loss or failure. Usually all data should be stored within a logical structure, so it is readily available to colleagues in your absence. Please see the Information & Records Management Policy for further details. The user's home drive on the network is specifically for information that has a requirement to be restricted. Specifically data should never be stored on the local "C" drives of a PC / unencrypted Laptop, or on the Windows "Desktop". The use of removable media (CD's / USB memory sticks) will only be possible following the acceptance of a clear business case and with the users agreement to follow strict controls over its use.

Where removable media is used with approval for archive material, then users should ensure that at least two copies are made of the media, these are stored in separate locations, are properly labelled (inc disposal dates) and that the storage of this media enables FOI and DPA requests to be serviced as required (i.e. an appropriate index exists). In the case of "Protected" or "Restricted" information, physical security is critical as the data is no longer protected by a network password. Individual file passwords should be avoided due to the susceptibility of their loss. If absolutely required then a note of the password should be made, placed in a sealed signed envelope and deposited in a secure area where senior management can gain access if required in your absence. If archiving electronic files for an extended period (greater than 5 years), please seek specialist advice from Information & Records Management section to ensure long term readability of the data.

Because of the above and the fact that removable media represents a high risk with regard to virus infections and unauthorised data removal/transfer, it is council policy to actively restrict the availability of removable media. This will be achieved via a mixture of a limited number of workstations with such facilities and restricting facilities to only those users with a genuine business case for such devices. Where removable media is allowed, ICT will often specify further technical functionality such as encryption.

## Confidentiality of Data

All computer users must make themselves familiar with the Council's Information Governance and Security Policy. In particular they must pay due regard to the confidentiality of personal data and ensure that "Protected" or "Restricted" data is not sent or disclosed to any unauthorised recipient. Employees must not establish a database containing **any** personal data without the prior authorisation of their line manager, the Corporate Information & Records Manager and ICT. When data classed as "Protected" or

“Restricted” is sent or transferred, this must be in a suitably secure manner and via a traceable delivery route. E-Mail rarely meets this requirement and should therefore not be used for the transfer of such data without previous written authorisation from the Corporate Knowledge and Information Manager.

## Unauthorised or Unlicensed Computer Software

Only approved, legal computer software may be used with council ICT systems. All software (and hardware) has to be purchased and approved by the ICT service unless written permission is given to the contrary.

On no account must users attempt to purchase or install software themselves. This includes commercial demos/trials, screensavers, shareware / freeware / OpenSource or software downloaded from the internet (including unlicensed music or video material) or drivers to connect devices (such as iPod’s or phones) to your computer.

Users should also note that unless explicitly authorised in writing by ICT, the use of Microsoft Access within the organisation is forbidden.

Violation of the above policy is liable to be considered as gross misconduct.

## Unauthorised Computer Hardware

Only approved computer hardware may be used with council ICT systems. On no account must users attempt to purchase or install hardware themselves, irrespective of how it intends to be used. Only authorised hardware may be connected to the council network or to council computing hardware and this will not usually include consultants/contractors own laptops. Specifically users may not connect any personal equipment (e.g. MP3 players, phones, cameras etc) to council equipment. Where there is a corporate need to connect devices to equipment, this must be approved by the ICT service and will usually be performed by them.

Violation of the above policy is liable to be considered as gross misconduct.

## Virus Checking

All computers have a virus scan system. This software must not be disabled. Any difficulties or viruses identified must be immediately reported to the ICT ServiceDesk. Until the issue is resolved the user must not use their PC and must follow instructions issued by the ICT service.

All disks, CD’s, memory sticks and other data media which come from any external source (including from an employee’s home) must be explicitly virus-checked before any data is transferred from them onto a council system.

Failure to follow this aspect of the policy will be treated as a disciplinary offence.

Please remember that if you suspect a virus, please contact the ICT ServiceDesk. Do not forward any E-Mails you might receive warning of new virus outbreaks to others in the organisation as these are often false and confusing or even mechanisms to introduce a virus themselves.

## Working Away From The Office

As a general rule staff should avoid taking council equipment or data offsite and must seek authorisation from their manager before doing so. Please note that in the case of data this applies to information on laptop hard drives or transferred by means of E-Mail or removable media (e.g. CD’s and memory sticks). Where “Protected” or “Restricted” data is involved, staff must obtain written permission from the Corporate Information & Records Manager in addition to their line manager and comply with any conditions specified.

If taking council owned hardware offsite (e.g. Laptop, PDA and/or Projector), please ensure that where practical it is kept from public view at all times. This significantly decreases the chances of theft and robbery and thus the chance of personal injury. If basic precautions are not taken (e.g. leaving a laptop on view in the back seat of an unattended parked car), any subsequent loss will be considered a matter of gross misconduct.

Remote access to ICT systems is provided to staff (where there is a clear business case for such access) in accordance with the following guidelines:

Within Central Bedfordshire Council there are 3 types of employee remote worker. These are:

- Home worker
- Mobile worker
- Casual remote worker

### Homeworker

Definition
Member of staff spends greater than (or equal to) 50% of their contracted time (averaged over a month) working from home. Formal home working must be agreed by the employee’s line manager, HR together with ICT and is subject to specific guidance and a formal agreement that is issued on an individual basis.

Equipment allocation

- Corporate ICT department supplies, thin client terminal, 19” TFT screen, keyboard and mouse. Equipment will be locked down (no USB access, floppy drive or CD drive).

- A standard black&white laser printer to be supplied if business case is made. (User will have to verify their strict compliance to corporate policies if “Protected” or “Restricted” data is being processed and a shredder may also be provided.)
- Member of staff is paid an allowance to cover the cost of a broadband link as specified by ICT.

Mobile Worker

Definition
Member of staff spends greater than or equal to 40% of their contracted time away from the office (but not at home).

Equipment allocation

- Supply corporate laptop, tablet or appropriate mobile device with encryption and 3G card if appropriate.
- When in the office the unit will have connectivity to the corporate LAN, a docking station, 19” TFT screen, keyboard and mouse.
- No provision will be made for home use.

Casual Remote Worker

Definition
Member of staff occasionally works away from the office. Averaged over a month the person is away from the office less than 40% of their contracted time or (if all time away is spent working from home) working from home less than 50% of their contracted time.

Equipment allocation

- Standard desktop equipment for use in the office.
- When away from the office, access to corporate resources provided over the internet using the Citrix Access Gateway, using equipment supplied by the individual. This access will be restricted so that no corporate information can be downloaded onto the machine being used for access.
- Possibility of a “laptop pool” where member of staff can book a laptop to be used for short periods of time. (e.g. presentations off site)
- No allowance provided for connectivity.

.

# THE INTERNET AND E-MAIL

## Internet Access

Internet access is provided for business purposes only. Limited personal use is permitted outside of working hours (e.g. Lunch breaks & outside of flexi time), however employees are reminded of the need for breaks in computer usage to promote correct workstation wellbeing. Consistent or frequent usage during rest breaks is therefore strongly discouraged (especially for people who have high amounts of VDU usage as a significant part of their standard role). For the sake of clarity, personal use is never acceptable during core hours. Any personal use is subject the following rules:

- It is strictly forbidden to download any files from the Internet for personal use (This includes the "streaming" of files, music files, video files, pdf & word documents etc).

- It is strictly forbidden to use the Internet for personal financial gain, freelance commerce, gambling, visiting pornographic or entertainment sites or for conducting political activities. This includes postings to discussion groups, or for taking part in any activity which may compromise the Council's image and reputation as well as participating (as opposed to viewing) in online auction sites (e.g. e-bay).

- Use of Instant messaging software and facilities for personal use (such as MSN/Windows Live or Yahoo IM) is forbidden.

- If a user accidentally accesses an undesirable site they must inform their manager, so that this can be taken account of during any monitoring or analysis.

## E-mail

Users of council internal or external E-mail facilities must be aware of the following:

1) That an electronic mail message is not a confidential or secure means of communication, unless sent via the Government Connect system. This is especially true of E-mails destined for outside the authority.
2) External E-mail is neither an immediate nor guaranteed delivery mechanism despite its usual high performance.
3) E-Mail has the same legal status as other paper and electronic media. All E-mails sent or received from authority's systems are the property of the Council.

The users of council E-mail must abide by the following rules:

- E-mails should at all times be treated as permanent written records which may be read by persons other than the addressee, if the recipient chooses to circulate it or uses blind copy.

- Personal data which is subject to the Data Protection Act, relating to any of the Council's citizens, employees, clients or customers must not be transmitted to a third party by way of standard e-mail without their express consent except where it is implied for business purposes. Whilst E-mail may be acceptable for one to one communication, it is rarely acceptable for the transmission of bulk data, where that data is of a personal or sensitive nature. If in doubt about any of these points, users should contact the Corporate Information & Records Manager for guidance.

- Documents, website links or messages received by E-mail should be checked by the user for their likely authenticity and integrity, prior to opening. All unsolicited e-mails from an unknown source ("SPAM") should be treated with suspicion. No attachments or links should be followed in such instances without further investigation

- Users should be aware of the practice of "phishing" (fraudulent E-mails made to look convincingly official in nature). Please take additional steps to verify the authenticity of E-mails which invite passwords or personal data to be disclosed.

- Care should be taken that E-mails are only sent to appropriate recipients as reading e-mails can be time consuming and, therefore, a waste of the receiver's time when not entirely necessary. Specifically the use of group sending should be carefully considered before use and on no account should "chain" or joke E-mails be forwarded to others.

- System performance and efficiency may be affected if large (typically more than 5Mb) files are transmitted in E-mails. Such use should therefore be strongly avoided and either the files compressed and reduced in size first or alternative methods of file transmission considered.

- Users must review their e-mail directory at least once a week to ensure that they delete messages which are not required to be retained. Should regular housekeeping not be carried out this will result in users running out of disk space and the system becoming inefficient. If a user receives an attachment for business use, it is good practice to save it and delete it from the E mail. Users should note that there is a size limit for all council mailboxes of 400Mb. This will apply to all users irrespective of position held.

- All internet E-mails are unpacked and checked automatically for viruses and spam, as the E-mail arrives at the council. However this is not a guaranteed process and users are required to play their part in the process by treating unsolicited E-mails from unknown sources with suspicion and care.

.

- Just as with paper documents, E-mails may constitute records of organisational activity and therefore should be treated as such. Until the council completely converts to an Electronic Document and Records Management System, E-mails must be treated in the same way as paper documents and the same retention periods apply. Therefore, relevant E-mails must be printed off and filed or kept electronically in a structured manner. Retention schedules which reflect the business needs of each service section should be drawn up in conjunction with the Corporate Information & Records Manager. Please remember that this applies to actual E-mails as well as attachments, especially where corporate decisions or advice are being given or discussed. Such information is often subject to disclosure under the Freedom of Information Act until any formal specified destruction date is reached under an approved retention schedule.

- E-mail messages that are sent to external organisations via the Internet will automatically carry an authorised council disclaimer statement and corporate footer.

- Users must not use their council E-mail address for social networking sites (e.g. Myspace, Facebook etc), irrespective of business or personal use. Where there is a legitimate business use, this will be approved by both the corporate communications team and the relevant director and recorded as an exception on the user's declaration form.

- Employees may use the corporate E-mail system for occasional personal use, subject to the conditions below and providing the nature, frequency and other aspects (e.g. time taken) do not reach an unacceptable level that affect your performance of your role or that of your colleagues,

- If employees use the council E-mail system to send personal E-mails, then these must not contain any attachments and be text only. Additionally corporate E-mail addresses must never be used as "registration" or "contact" addresses for personal use on social networking sites, discussion groups or personal commerce transactions (for example - E-Bay, on-line retailers or personal banking). All personal E-mails received which contain an attachment must be deleted without the attachment being opened. The sender must be informed of the council policy to prevent further attachments being sent.

## E-MAIL ETIQUETTE

All users should be made aware that E-mails can often be retrieved even if they have apparently been deleted from the system. E-mail is as permanent as the written word and should be treated as such and can be relied upon as much as any other document admissible in law. The following principles must be taken into consideration when using or drafting messages/communications for transmission by electronic mail:

- All users must view their E-mail on a regular basis – ideally daily. If employees are not in the office, they must make appropriate arrangements for the handling of E-mail messages (e.g. proxy access, or setting up a rule to divert or respond to messages). Sharing of passwords is not an acceptable method of achieving this. If you are unsure of how to use proxy access or rules, then please consult the ICT Service Desk. Please note that when setting up (automated) rules never use “reply to all”, only “reply to sender”.

- E-mail should not be used as an alternative to face-to-face or verbal communication as this may prevent satisfactory dialogue between the parties.

- E-mail messages must never contain any words, phrases or other material which may be sexually or racially abusive or discriminatory, in any way whatsoever, or which may have the effect of the recipient feeling or experiencing harassment as a result of receiving the message. Consequently, improper reference should not be made to race, creed, colour, nationality, ethnic origin, age, language, religion, political or other opinion affiliation, gender, gender reassignment, sexual orientation, marital status, connections with a national minority, national or social origin, property, birth or other status, family connections, membership or non membership of a trade union, or disability.

- Care must be taken that the content or the subject of the E-mail does not cause offence in any way to the recipient, nor that it is defamatory. In particular, care should be taken with the style of the language used and the effect that the message will have on the recipient. In particular, where messages or words are expressed in capital letters this may be perceived by the recipient as the equivalent of shouting and is therefore very likely to cause offence. Unlike face-to-face communication, tone cannot be easily identified on an E-mail, so ironic, sarcastic, humorous or ‘clever’ comments should be made with care, as they can easily be misinterpreted or cause offence. Please remember material will be deemed as being defamatory if it has a lowering effect on any person or on the organisation.

- The onward transmission of E-mail messages which contain offensive material, pictures or comments is strictly forbidden. This includes onward transmission to the IT service or even the Police. Should such material be of an illegal nature, it should not be forwarded or deleted, but your line manager and the ICT section notified immediately.

- Employees who receive an E-mail which causes offence should follow the standard council Bullying and Harassment policy.

- Employees who are concerned, or believe, that an E-mail they intend to circulate may be inappropriate, should not circulate it. If in doubt, they should refer the matter to their manager/supervisor who should vet the E-mail before it is published or circulated. Please remember to err on the side of caution

- Employees should also be careful that they do not breach any copyright in pre-printed or published material that they incorporate into their e-mails for transmission to third parties or for general publication. It is expressly forbidden to copy, download or transmit to third parties any published material that has been written by other people without their consent (including scans of newspaper or magazine articles). This will also leave the Council open to legal action by the owner of the copyright. Employees who are concerned, or believe, that an E-mail they intend to circulate may contain copyrighted material, should refer the matter to their manager who should vet the E-mail before it is published or circulated.

- Employees should, at all times, exercise a general duty of care with respect to the drafting of E-mails, insofar as the e-mails will clearly be circulated or published for, or on behalf of the Council. The reputation and business interests of the Council are at risk by the careless use and abuse of the E-mail and Internet by any of its employees. You should not give the impression that your message represents the opinion of the Council unless appropriately authorised to do so.

- When wording E-mails, take time to review them before sending. Be particularly careful of responding when upset or angry as the immediacy of the medium can allow you to respond inappropriately in a manner you might later regret.

- When responding to E-mails, do not "reply to all" unless everyone in the original message really needs to see your reply.

- Only copy those people on E-mails who really need to know the contents of the communication. Frivolous or lax use of inappropriately copying large numbers of people on E-mails is actively discouraged.

- Users should in general avoid using E-mail for notices and information distribution, unless it is of a particularly important, confidential or urgent nature. Generally the Intranet is the most appropriate place to provide information to a large number of colleagues.

- When sending E-mails (particularly group E-mails), consider using an expiry time (whereby any unread copies of the mail in people's inboxes are automatically deleted after a given length of time or after a specific point of time). Examples of this may be an information E-mail relating to a specific event, which will have no validity after that event has passed.

- When away from the office do use a rule to inform senders of your absence, the expected date you will deal with their reply and if appropriate an alternative contact for urgent enquiries. Please note that when setting up (automated) rules never use "reply to all", only "reply to sender".

- Whilst the use of individual E-mail addresses (i.e. forename.surname@centralbedfordshire.gov.uk) is generally fine for day to day communications (e.g. letters), avoid their use in general Central Bedfordshire publications (paper or otherwise). Consider the effect any change of personnel might have on the validity of the document. It may be appropriate to instead talk to the ICT service about a generic service based address in publications that are expected to have long validity periods.

- Learn and make appropriate use of E-mail & calendar sharing and delegation functionality and the associated classification of E-mails/diary entries (e.g. private).

## DATA STORAGE (inc Digital Photographs)

With the advent of large cheap disk drives in personal computers, issues of data storage are often now not adequately considered by users. The fact remains that the data storage, business continuity, backup, archiving and performance considerations of corporate data storage means that this area is still a very costly activity and one that needs to be considered by all users.

The general concepts of good practice that apply to paper storage equally apply to electronic data storage and need to be followed, namely:

- Data should be held in accordance with a defined and agreed retention policy. Any unwanted data outside of its retention period should be deleted. Data within a valid retention period but that is of a historical and rarely used nature, should be archived from live systems in an appropriate manner. Please contact the corporate Information & Records Manager for advice.
- Data should be stored in a consistent and organised way
- Data should be held with the appropriate level of security
- Data should be only held once and important data version controlled. (Multiple copies waste space and can lead to problems with a lack of authoritative versioning of documents)

Particular attention needs to be paid to image files (be they digital photographs or scanned paper documents). This is because these files can be extremely large and are often stored at a quality “resolution” far in excess of that which is needed. Users involved in the creation, manipulation or storage of these files must ensure they are aware of the best practice in this area.

Consideration should also be given as to the format in which to store data. In particular the following should be considered:

- Future requirement to enable (or prevent) people from editing the document
- Audience accessibility to document and it’s contents
- Internal or external audience
- File size
- Access to file in electronic format (if over five years from present)

If you are unsure please contact ICT for further guidance and advice.

## Business and Personal Use of Central Bedfordshire ICT Systems

Dear {employees name}

As you will have access to Central Bedfordshire Council ICT systems for business and limited personal use, we require you to sign and return this letter to Human Resources. By doing so you certify that you have read and understood the approved acceptable use policy relating to ICT systems at Central Bedfordshire Council and agree to abide by this policy both in terms of your business and any personal use.

This is to safeguard Central Bedfordshire Council's greater interest, and to ensure the effective operation of our computer, telephony and related systems.

You should also be aware that Central Bedfordshire Council reserves the right to monitor e-mail and Internet usage in compliance with the appropriate legislation.

Thank you for your co-operation in this matter.

Yours sincerely

*Chief Executive*

*Name of Employee*

I confirm that I have read and understood and will abide by the Central Bedfordshire ICT Acceptable Use Policy. I accept that my usage of ICT systems will be monitored from time to time and that I have no expectation of privacy as a result of any such usage.

Signature: ______________________Date: ___________

<With exceptions as agreed by Directors as attached.>