INFORMATION MANAGEMENT AND

TECHNOLOGY (IM&T)

SECURITY AND CONDUCT POLICY

Information Management and Technology (IM&T)

Security and Conduct Policy

1 Aims of the Policy

1.1 This policy document establishes the IM&T Security and Conduct policy for Winchester City Council (the Council) to safeguard information and processes associated with electronic information and communication systems. This Policy also assists in promoting computer security awareness within the Council and encouraging reasonable and well-informed behaviour as well as good management practice.

1.2 This policy is designed to:

i) Safeguard information, processes, behaviour and conduct associated with electronic information and communication systems both within Council policy and the wider legislative framework.

ii) Assist in promoting computer security awareness within the Council, maximising the advantages that Internet and e-mail access bringwhilst seeking to minimise the associated legal risks and practical hazards.

iii) Encourage reasonable and well-informed behaviour as well as good management practice. The Council's policy is for members and staff to be familiar with the Internet, e-mail and other electronic facilities at their disposal so that confident, skilled users are developed.

1.3 Any breach of this Policy by staff may lead to disciplinary action being taken and, in cases of gross misconduct, termination of employment. Any breach of this Policy by Members may be referred to the Standards Committee. Any breach of this Policy by contractors will be subject to appropriate action by the relevant Head of Division.

2 Scope

2.1 This Policy applies to all Council personnel, temporary staff, agency staff, contractors, consultants, suppliers and Councillors who use any Council information or communication technology, on site or away from Council premises.

3 Infringements of Policy

3.1 Infringements of this Policy may warrant disciplinary action and, in cases of gross misconduct by staff, termination of employment without notice. In particular, attention is drawn to the following infringements:

i) Viewing, creating, circulating, distributing, storing, downloading or printing material that might be offensive, illegal, pornographic or sexually explicit, that brings the Council into disrepute or that exposes it to legal action. For staff, such action is likely to be considered as gross misconduct and, if so, would result in termination of employment without notice. The Council reserves the right to recover defamatory material and use it as evidence against an individual.

ii) Using communication facilities for purposes that may be illegal or contravene Council policy such as disclosing official information without authority.

iii) Hoaxing, hacking or damaging Council or other networks, or knowingly using unlicensed software.

iv) Using communication facilities (landline, mobile or email) for unreasonable extensive private use contrary to the provisions of the guidance given in sections 14 and 16 of this Policy

4 Responsibilities

4.1 **All** users are responsible for ensuring that they comply with this Policy. A pop-up box appears at logon stating that, by logging on, users agree to accept the terms and conditions of this Policy when entering the Council's network.

4.2 Under Government guidelines all users of the network will be required to sign a document stating that they have read and understood the Information Security Policy. The policy must be reviewed no greater than six monthly intervals by the policy owner.

4.3 **The Head of IM&T** will ensure:

i) Review this Policy annually, in consultation with the Head of Organisational Development and issue minor amendments as necessary.

ii) Develop and publicise this Policy and inform staff and members of IM&T related security issues.

iii) Develop administrative, physical, and technical security controls to meet the Council's IM&T security objectives including access control, cryptography,

networks and communications, malicious code and attacks, analysis and monitoring, operations and administration and risk, response and recovery.

vi) That all changes to this policy are communicated to Heads of Division.

vii) Keep a record (audit trail of the detail of policy applicable to any point in time in the past two (2) years.

4.4 **The Head of Organisational Development** will ensure:

i) Provide a copy of this Policy within the Induction Pack issued to new staff.

ii) Ensure that induction training courses outline the key elements of this Policy, provide general guidance on the use of electronic systems and cross-reference these security policies with the Council's Equal Opportunities Policy.

iii) Provide IM&T with a list of Starters at least 5 working days before start date, Leavers at 5 working days before their last working day and of staff changing duties at least 5 working days before the change takes place, so that user information is kept up to date,

iv) Advise IM&T IT Service Desk of any member of staff who has been given permission to work from home or be a mobile or flexible worker.

v) That all staff given access to the secured Council Network will have signed a copy of the IMT Security and Conduct Policy – Employee Summary prior to being granted access to the system.

4.5 **Heads of Division** will ensure that:

i) This Policy is transmitted to all staff, contractors, consultants and agency staff within their Division and to all Members and that attention is periodically drawn to the need to comply with the policy or to changes.

ii) The procedures within this Policy are complied with and appropriate security measures are established and maintained with regard to access to Council databases and other electronic information systems or resources.

iii) IM&T is advised of any members of staff who have been given permission to work from home or be a mobile or flexible worker.

5 Security - Monitoring of System Usage

5.1 The purpose of monitoring is to:

i) Record personal use of e-mail and Internet services that may be costly and can affect the efficiency of the network system as a whole.

ii) Ensure usage of the systems does not disrupt or damage the performance or reputation of the Council.

5.2 The Council will record the use of all of its IM&T equipment, in particular the use of the Internet and the contents of mail and file transfers, irrespective of whether they are for Council or private use. Internet monitoring shows which sites are accessed, by whom, when and for how long. This evidence may be used during a disciplinary investigation.

5.3 Reports will be made available to Heads of Division who are responsible for taking appropriate action. Where necessary the Head of IM&T, the Head of Organisational Development, Head of Legal and Democratic Services or the Chief Executive will advise on the suitability of material, investigate web sites or seek the opinion of the police.

5.4 The Council reserves the right to access data files held within personal folders or password protected files in connection with the legitimate business of the Council.

5.5 The content of e-mails (both incoming and outgoing) will only be accessed where specific circumstances justify this action. All such monitoring will be carried out for legitimate purposes only and in accordance with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Monitoring will take place on a monthly basis and Heads of Division will be provided with this information and which they will act upon as appropriate.

6 Hardware and Software

6.1 All IM&T hardware over a value of £XXXX will be registered, when procured, with a unique asset number recorded on the Council's asset register.

6.2 Users should not move PCs, printers, scanners or other IM&T equipment as this must be done only by the Council's IT&T staff unless otherwise agreed.

6.3 No hardware, such as printers, PDA's or laptops, should be physically connected to the Council's network without the authorisation of IM&T using the agreed 'Change Control' procedure.

6.4 Good management procedures must be followed in relation to all equipment. Specifically:

i) Council-owned portable laptops/tablets and computer accessories must be stored in a locked cabinet when not in use, except when kept at home.

iii) Any sensitive data saved on the hard drive must be removed or deleted by the user when portable equipment is returned.

6.5 The disposal of surplus and obsolete IT equipment must be carried out by IM&T.

6.6 All software packages used on Council owned, leased or rented computer systems, including copyrighted freeware and shareware, must be registered in the Council's inventory managed by IM&T prior to installation.

6.7 Users must observe copyright and licensing agreements. Software is usually licensed only for a particular number of users. If anyone is unsure how many copies of software are licensed for their use, they must seek advice from IM&T. Advice on licensing may be sought from IM&T. Licensing agreements vary and individuals are responsible for understanding and abiding by the terms.

6.8 No software should be loaded on Council equipment except by the Council's IM&T staff. All such software must be purchased or obtained by IM&T and with the approval of the appropriate Head of Division.

6.9 No software should be downloaded from the Internet except by the Council's IM&T Staff or without permission from IM&T. It must be virus scanned before it is loaded and used. All licensing requirements, payment conditions and deletion dates associated with downloaded software must be met.

6.10 All software, hardware and electronic equipment must be purchased through IM&T who will ensure licensing agreement forms are filed with the supplier. Registration may provide the basis for getting assistance from the manufacturer if the software is lost, stolen, or damaged.

6.11 Staff must use only those electronic resources that have been authorised by their manager. The use of Council equipment for unlawful purposes, including the installation of fraudulently or illegally obtained software, is strictly forbidden and will lead to disciplinary action being taken.

6.12 Users must switch off PCs, screens and printers when going home or when leaving them unattended for some time.

6.13 The computer suite must be locked and access through a coded key pad that is changed every 30 days. Any access to the computer suite should be recorded and monitored by the IM&T Client Officer.

6.14 When a member of staff leaves the employment of IM&T, the access code to the computer suite must be changed immediately and the Head Of IMT informed. A risk assessment must be carried out and consideration to system passwords may also be changed.

6.15 All data must be secured and backed up by IM&T. All backups MUST be stored offsite in a secure location.

6.16 The spare keys used by IM&T for the fire safe, cabinets etc, must be stored in an offsite location.

7 Working from Home/Mobile Working

7.1 Additional arrangements apply to staff using Council IM&T equipment or services from home or when mobile.

All authorised remote access will be via WCC's approved methods using a minimum of two of the three factor authentication methods.

The three factors of security are:

- What you are
- What you own
- What you know

Mobile and Remote access is via the published VPN web front end, https:\\portal.winchester.gov.uk

Access through the published VPN front end is via a dual factor authenticated logon using WCC's cyrpto card key fobs only. No other method of remote access is permitted.

Dual factor authentication methods consist of User name & Password (Active Directory) and Unique ID Tokens that generate an eight digit number that needs to be included at the time of access.

7.2 Laptops and other portable devices:

i) Must not be left unattended in public places

ii) Must not be left in a car overnight

iii) Must be kept in the locked boot of the car and out of sight when left unattended at other times.

7.3 Use of Council equipment is restricted to Council business only unless permission is given from the Head of IMT There may be personal tax implications if equipment is used outside council purposes and advice should be sought.

7.4 Data accessed from home or when mobile should be treated with the same confidentiality as data accessed in the office. Equipment and data should not be left unattended.

7.5 Those working from home should familiarise themselves with the Council's Home Working Policy and sign if necessary.

8 Third Party Remote Access

8.1 Any service or application administrators that require third party remote assistance must seek prior approval from the IMT Department. No other remote access method is permitted other than that agreed and adopted by the Business.

8.2 All third parties need to comply with the Council's security & conduct policy**.**

8.3 Remote access is available between 0800hrs and1700hrs, Mon to Friday. Any remote access requirements that fall outside of these hours are only available if pre-arranged, contact the IT Service Desk for assistance on 01962 848515

8.4 The necessary remote access form needs to be completed by the third party in question, details of which can be found at

http://ntserver7/intranet/finance/itclient/index.htm

Permission will only be granted to access Winchester City Council IT systems remotely if the above form is completed to the satisfactory level. Permission will be limited to the servers specified on the completed form and any attempt to access other areas will be classed as an attempt to breach security. Suppliers should also be made aware that that all information accessed is confidential and should not be disclosed to any other party without prior permission from Winchester City Council.

Further details can be found on the Intranet

9 Data and Files

9.1 Physical access by non-authorised personnel to the Council's electronic equipment is strictly forbidden.

9.2 Unattended computer terminals must be password protected either by being at a logon prompt or by a password protected screen saver.

9.3 All employees must be alert to the presence of any non-authorised personnel in the vicinity of computer equipment.

9.4 All files must be stored on a server and items only downloaded to a laptop for a specific reason and then uploaded to the server if any changes to documents. The use of version control must be used on all documents to ensure that the latest version of the document is being used.

9.5 Personal information must not be saved on any non-encrypted hard drives or external devices (i.e. USB, CD or any other media format). Data must not be stored locally on computer hard drives.

9.6 Confidential or sensitive information should be kept securely on the server. Any paper based document with sensitive information must be locked in a secure cabinet when not being used.

9.7 Any personal data being shared with a third party must either be encrypted and password protected. If password protected the password must be sent in a different document than the actual data. Advice on encryption and password protection should be requested from IM&T. Care should also be taken to comply with data protection principles in the Data Protection Act. Sharing of personal data with a third party should always be approved by the individual's line manager. Advice can be obtained from the Legal Division and IMT.

9.8 Email sent over the Internet is not encrypted as standard and as such, any communication with private email accounts is not recommended. IM&T cannot guarantee the integrity of any data exchanged over the Internet. All data sent via this communication method is at the data owners own risk and should only be used if alternative methods of communication are not available. If in doubt contact the IMT Security Officer.

9.9 Any impact level 3 (IL3) restricted information must be emailed via the PSN Government Connect Gateway. Advice on this process is available from IMT.

9.10 Reports and customer data should not be left lying around where unauthorised access may be readily available.

9.11 Data accessed from home should be treated with the same confidentiality as data accessed in the office.

9.12 Unauthorised access to data and files is forbidden.

10 Passwords and Logons

Always maintain the secrecy and confidentiality of your password to ensure its integrity as an authentication method. The following practices are necessary to maintain password secrecy:

10.1 All users of any Council computer system must be issued with an individual password and logon.

10.2 Users must adopt sound password practices, general good practise includes:

- Under no circumstances should an account password be divulged to another user, including the IT Department. If a request is made for your password then you must alert the Head of IMT, or delegated authority, immediately.
- Avoid recording your passwords in an insecure manner, in any form, personally encrypted or otherwise.
- User passwords must be changed every 60 days and main system passwords every 30 days.
- Avoid saving passwords in Web browsers and other applications. Passwords should not be saved and option boxes for saving passwords should not be ticked.
- Always delete e-mails that contain a password. Always change passwords that are automatically assigned to you.
- Passwords should be a minimum of eight characters and must contain at least three of the following characters: upper case, lower case, digits and symbols, unless there are system constraints.
- Passwords cannot be reused for twenty changes.
- Where a user has left the employ of the authority or is on long term leave, including maternity leave, and another user requires access to that user account approval must be given by the joint Head of IT and relevant Service Head prior to access.
- If temporary passwords are required these must be changed or deleted as soon as possible. Temporary passwords must be conveyed to users in a confidential manner.
- Use a Web site's logout feature rather than just closing your browser.
- Avoid using common passwords, common phrases, or dictionary words. Avoid getting too attached to a single password. Be smart with secret questions and answers.
- Never reuse the same password more than once, especially among different systems.
- Avoid passwords that include personal dates or other significant numbers, pet names, relatives or loved ones, vehicle names, favourite sports teams, or

other personal information. Avoid words or numbers relating to yourself or your environment.

- Avoid using words connected to you that might lead to reuse. Avoid using predictable patterns or sequences.

10.3 Users must use only their own user name and password to access any system.

10.4 Users must not allow anyone else to use their user name and password. This is not only a security risk but could lead to false accusations of misuse as monitoring of the Council's Internet usage is based on user names.

10.5 Users must not attempt to find out the password of another user.

10.6 Outside suppliers dialling in remotely to the Council's network to support applications are not required to have individual user names and passwords but must complete a Change Control form which is authorised by IM&T Client Officer.

10.7 A corporate screen saver should be activated after 15 minutes and users must enter their password to unlock the screen.

10.8 Where laptops are used for home logons the password file must not be saved (i.e. the dialogue box indication to save the password should not be activated) in order to prevent unauthorised access if the laptop is lost or stolen.

10.9 If any crypto card key-fob is lost or misplaced this must be reported to IM&T Client Officer immediately. Access to the Network will not be possible without the 'key-fob'. A charge may be incurred to the individual or department of the lost crypto card.

11 Security Incident Reporting

11.1 Any user who feels their password security has been compromised should change their password immediately and report the incident to IM&T.

11.2 Any user who feels that malicious damage may have been caused by someone using their user name and password should report the incident immediately to their Head of Division and IM&T.

12 Computer Viruses

12.1 All mail is filtered by a third party anti-virus, spam and content filtering software solution and anti-virus software is running in the background on all Council PCs.

12.2 Users should ensure that they are aware of the nature and danger of computer viruses and should take all care to ensure that they are not introduced to the Council's computers or its networks.

12.3 Viruses are most frequently spread via the downloading of files from the Internet, through the use of an infected USB or CD or by attachments to email messages.

12.4 The use of floppy disks, USB's and CDs are restricted, approval for the use of such devices must be agreed through a risk assessed business case by Heads of Division and IM&T

12.5 To reduce the chance of getting a virus, users should virus check all USB's and CDs before use. Software should only be downloaded from the Internet by the Council's IM&T staff. **ALL suspected viruses must be reported to IM&T immediately.**

12.6 All users are responsible for ensuring that the Council's anti virus software is not removed from the PCs.

12.7 Users should not circulate information they might have received about virus or hoax software. Any information about virus warnings should be given to IM&T who will check the information and issue a message to all users if appropriate.

12.8 Users should be cautious about opening email and associated attachments from an unknown source. Any suspicious emails should be referred to IM&T.

13 Hoaxes

13.1 There are many virus hoaxes that claim falsely to describe an extremely dangerous virus. They use pseudo-technical language to make impressive-sounding, but impossible, claims. They claim that the report was issued or confirmed by a well-known company and ask you to forward it to all your friends and colleagues.

13.2 Users must not pass on warnings of this kind, as the continued re-forwarding of these hoaxes simply wastes time and email bandwidth.

13.3 Hoaxes via email may come with a file attached. Such attachments should be treated with caution as they may be infected with a virus. Any user found to have distributed hoax information intentionally via any Council communication system will be subject to disciplinary action.

13.4 Other hoaxes that are scams designed to deceive people into parting with money also circulate. Users should be vigilant and pass any suspected hoax e-mails to IM&T who will investigate and issue a warning as appropriate to all staff and councillors.

14 Conduct - General Use of Equipment

14.1 The Internet, use of e-mail and text messaging now has a substantial presence throughout the world. As a consequence of e-mail, Internet and other electronic activities, defamation and harassment action, negligence cases, breaches of copyright and claims in respect of disclosure of trade secrets and personal information have arisen.

14.2 Council electronic equipment and software should be used in a responsible, legal, and ethical fashion. Users must not take any action that could bring the Council into disrepute, cause offence, interfere with Council work or jeopardise the security of data, networks, equipment or software.

14.3 Council computer equipment and software, as well as telecommunication services and other electronic equipment are for Council business purposes. Occasional personal use by staff is permitted at the discretion of line managers provided it does not interfere with Council work, is not conducted in Council time, conforms to this Policy and is not associated with personal business interests. Similarly, Members may use Council equipment for occasional personal use and for Council and ward matters. However, Council equipment must never be used to promote support for a particular political party nor for conducting personal business interests. Council equipment must only be used by council employees or members. It can be used for communication within political groups in the Council in connection with the proper conduct of Council business.

14.4 The removal of Council owned software and hardware for personal use, whether done by copying or by removal of the master software, is prohibited and illegal under the Council's contracts with the vendors.

15 Workstations – Health and Safety

15.1 Risk assessments must be carried out within each Division on workstations used by staff. Help on this can be obtained from the Council's Health and Safety Officer.

15.2 Users should ensure they are familiar with the Council's policies on Health and Safety with regard to workstations, either in the office or at home.

16 Messaging (Telephone, mobile and email)

16.1 Messaging means communications made by email and telephones, including mobile phones, and includes text and media messaging.

16.2 Messaging, whether sent internally or via the Internet, should be regarded as public and permanent. It is never completely confidential or secure and, despite its temporary nature, it can be stored, re-sent and distributed to large numbers of people.

16.3 Messaging must not be used for sending offensive, threatening, defamatory or illegal material. Messaging can be the same as sending a letter or publishing a document in law, so defamatory comments could result in legal action.

16.4 Managers should be particularly careful what they commit to messaging. It can be used as evidence in industrial tribunals and formal enquiries, including internal disciplinary and grievance hearings.

16.5 It is poor practice to use messaging to criticise or rebuke staff. Such matters should only be discussed face-to-face.

16.6 Messaging must not be used to harass staff or other recipients. Harassment can take the form of argumentative or insulting messages (flame mail) or any other message the sender knows or ought to know would cause distress to the recipient.

16.7 Users posting information to newsgroups should not include any information that brings the Council into disrepute or that promotes support for a particular political party. Including a disclaimer may not be sufficient.

16.8 It is easy to be misunderstood in messaging. People forget that the emotional meaning is often lost in text. Humour can be misinterpreted. Email and text messaging should be unambiguous. Neticons (symbols such as ☺ used to show humour, sadness or anger) are not widely understood and should not take the place of a clear message in plain English.

16.9 Every user has a mailbox limit - that is, there is a restriction on the volume and size of e-mails that can be held in Received, Sent and Deleted boxes. Each user should maintain good housekeeping arrangements by deleting e-mails frequently in each of these areas or by saving them to either their filing structure on the server or within the EDRM (Electronic Document and Records Management system). If housekeeping is not carried out regularly by the user, they will receive a message warning them that their limit has been reached. In some cases e-mail may not be received or sent until housekeeping is done. If this causes problems IM&T should be contacted.

16.10 To reduce the problems associated with mailbox limits, care should be taken when sending large files. In addition to causing problems with both their mailboxes and the recipient's, transmission of large files can slow down the network and impede the work of others. Recipient email systems are rightly suspicious of graphical attachments and therefore your email might not get through.

16.11 The email and telephone system is for business communication: thus personal messages unconnected with work should be kept to a minimum. The Council expects all members and staff to adopt a common sense and reasonable approach to the use of such facilities. Staff should conduct any personal messaging in their own time.

16.12 Personal use of the Council's messaging systems is permitted for exceptional reasons such as an immediate need to contact the emergency services, or in the case of a domestic emergency, for example a family illness or changes to carer responsibility arrangements. Such messages should be kept to a minimum and wherever possible be carried out in the staff member's own time.

16.13 Staff are not permitted to use the telephone system for international or high rate premium number calls unless permission is sought from Head of IMT, Director or Chief Executive.

16.14 Those with Council mobile phones should arrange to have a second line connected for personal calls. Personal calls or text messages should not be sent from the primary line.

16.15 Winchester City Council operates an email push facility to authorised users using WCC mobile devices only. Delivery of WCC push email to non WCC mobile devices is strictly prohibited. Access to WCC mobile devices is subject to WCC's mobile working policy and associated authorisation.

16.16 Emails and telephone messages (either verbal or text) which are, or may be considered to be, insulting, defamatory or libellous or which are contrary to the Council's Equal Opportunities policy are forbidden whether or not the person who is being insulted, defamed, libelled or discriminated against is likely to see the contents of the message.

16.17 Personal or confidential information should not be divulged over the telephone or by email without verifying the identity of the recipient independently. For example, although an e-mail address may state an individual's name, it may have been set up by another person. Care should also be taken to verify officers' or councillors' private e-mail addresses, if an e-mail address outside the Council's system is being used.

16.18 Users must not use Council e-mail or telephones to publish confidential, critical or defamatory information about the Council or any other organisation or individual. Sending emails or using a telephone in contravention of this policy may be considered gross misconduct and may result in summary dismissal for staff. Members contravening this policy may be referred to the Standards Committee.

16.19 The Council undertakes regular monitoring of telephone and Internet usage via system generated reports. Senior Management is provided with regular reports on costs and times of calls and times and details of access to internet sites. Results from such monitoring may be used during a disciplinary investigation if such usage is outside the permissible uses outlined in this policy.

16.20 The Council reserves the right to monitor the use of emails, telephony and the internet for the purposes of enforcing this policy in accordance with the

Telecommunications (Lawful Business) (Interception of Communications) Regulations 2000.

16.21 Should the Council be sued due to misuse of Council IM&T equipment or the actions of a user that contravene this policy, the Council reserves the right to claim damages from the user concerned.

17 All Staff Distribution List

17.1 Following approval, as per section 3.1, use of the_ All Staff distribution list is restricted to the following:

i) Urgent messages relating to work (for example: requests to find out who wants a particular invoice that has been received in the wrong division)

ii) Urgent messages relating to the Sports and Social Club activities (for example: advertising spare tickets for a social event)

iii) Messages from UNISON issued through the Branch Secretary

iv) Other messages must not be sent to all staff without the prior approval of a Head of Division or IM&T.

17.2 General information to staff, Members and contractors, including advance notice of social events, should normally be given through City Voice or the Members Briefing Note and should be sent to the Council's Corporate Communications Manager.

17.3 Any person who has information that they feel should be distributed to all staff (for example: a warning about cheque fraud in the area) must speak to IM&T and the communications team who will check the information and issue a warning if appropriate. This is to ensure that those receiving messages are clear that they are genuine and not a hoax.

18 Internet Use

18.1 When using the Internet, social network sites or bulletin boards, the following guidelines should be adhered to:

i) Job-related details from approved sites e.g. from .gov.uk sites, may be downloaded.

ii) Downloading of any program or update to programs must be done only by an authorised member of IMT due of the high risk of infecting a system with a virus. Downloading games or software to Council equipment is expressly forbidden unless previously authorised by the Head of IMT or delegated authority.

iv) Postings made to bulletin boards should not contravene Council policies nor damage the Council's reputation.

v) Loading of any information onto the Intranet or Internet that may be detrimental to the Council is prohibited.

vi) The Council will block any Internet site that is deemed unsuitable e.g. pornographic sites.

vii) The Council will also block any sites that are being used excessively during core hours. Access to sites may be authorised during lunch hours, before and after core hours.

18.2 **Social Networking Sites**

Social networking sites rely on connections and communication, so they encourage you to provide a certain amount of potentially private or corporate information. When deciding how much information to reveal, people may not exercise the same amount of caution as they would when communicating with someone in person because

- The internet provides a sense of anonymity.
- The lack of physical interaction provides a false sense of security.
- They tailor the information for their needs.
- They want to offer insights to impress potential customers or associates.

While the majority of people using these sites do not pose a threat, malicious people may be drawn to them because of the accessibility and amount of potentially private or corporate information that's available. The more information malicious people have about you, the easier it is for them to take advantage of you.

Using excessive information provided about corporate email addresses, management structures and contacts names, a malicious person could impersonate a trusted associate or convince you that they have the authority to access other private, corporate or financial data.

Additionally, because of the popularity of these sites, attackers may use them to distribute malicious code. Sites that offer applications developed by third parties are particularly susceptible. Attackers may be able to create customized applications that appear to be innocent while infecting your computer or sharing your information without your knowledge. To protect yourself and the Council:

- Limit the amount of personal information you post
- Remember that the internet is a public resource
- Evaluate your settings
- Be wary of third-party applications
- Check privacy.
- Keep software, particularly your web browser, up to date
- Use and maintain anti-virus software

19 Offensive, Illegal, Pornographic and Sexually Explicit Material

19.1 Offensive material is anything that is pornographic, involves threats or violence, and promotes illegal acts, racial or religious hatred, or discrimination of any kind. It also covers sending material which the person knows or ought to have known could offend colleagues or other recipients with particular sensitivities, even if it is not explicitly offensive, for example, religious or pro-hunting views.

19.2 Anyone using Council equipment for such material may face serious disciplinary action. If illegal material is accessed, the Council will inform the police and criminal action may follow.

19.3 Often when accessing a harmless site, links are automatically made to other sites or pages, and these could be inappropriate. Anyone accessing such sites accidentally should inform their manager and IM&T within twenty four hours. Accidental access will not result in disciplinary action, but failure to report it could do so.

19.4 People receiving offensive or sexually explicit material should inform their manager and IM&T immediately. Such material may not be identifiable until opened and, in these cases, individuals will not be held responsible provided they report it within twenty fours hours.

19.5 People receiving hate mail or emails asking for money should refer these to IM&T immediately and HR should be informed.

19.6 Any user who accidentally encounters offensive material on the Internet, or who is sent offensive material via e-mail or any other means, or witnesses the accessing of offensive material must report the incident to their Manager and IM&T within twenty four hours.

19.7 Individuals who bring their own laptops, other electronic devices or external storage devices into the workplace containing illegal or offensive material will be treated in the same way as those using Council equipment. Similarly, those who use their own equipment to connect to the Council's network remotely and who use that connection in this manner will be treated in the same way as those using Council equipment.

19.8 On occasion staff may need to access such sites in undertaking their duties, but before doing so they should obtain permission from their Manager or Head of Division and IM&T must be informed. Each site visited will be recorded in a log which identifies the site and the date and time of the visit. The log will be reviewed regularly by the Head of Organisation Development and Head of IM&T. Except in these circumstances there can be no possible legitimate Council use for accessing or transmitting sexually explicit materials at work. The accessing, viewing, downloading, storing or printing of any content of an illegal, pornographic or sexually offensive nature is expressly forbidden and will be treated as gross misconduct

leading to summary dismissal for staff or, for Members, to a report to the Standards Committee.

20 Government Connect

20.1 What is PSN (formerly GCSX)?

PSN stands for Government Connect Secure Extranet. It is a secure, private network. All local authorities in England and Wales are currently connected to PSN and the service can also be used by other public sector organisations that have a requirement for sharing information securely with local government and central government departments and agencies. PSN forms part of the Government Secure Intranet (GSi), which is the collective term used for the various Government networks that are all connected together. The PSN can be used to securely share data between local authorities, central government departments and other organisations that connect to the GSi such as the Police and NHS.

20.2 What Should I Send via the PSN

Personal data must not be sent by insecure means such as open emails. An item or groups of items of data are regarded as 'personal' if it is possible to identify an individual from it.

20.3 What is personal data?

Data Protection Act 1998 – in short

If you hold information about individuals either on computer or in certain types of filing system you may be holding ‘personal data’. Broadly speaking the DPA covers four types of information (referred to as ‘data’ in the Act):

(i) Information processed, or intended to be processed, wholly or partly by automatic means (that is, information in electronic form usually on computer)

(ii) information processed in a non-automated manner which forms part of, or is intended to form part of, a ‘filing system’ (that is usually paper records in a filing system)

(iii) information that forms part of an ‘accessible record’ (that is, certain health records, educational records and certain local authority housing or social services records, regardless of whether the information is processed automatically or is held in a relevant filing system) and

(iv) Information held by a public authority (referred to as ‘category ‘e’ data’ as it falls within paragraph (e) of section 1(1) of the DPA).

In most circumstances it will be fairly easy to decide whether the information you hold falls within one of the four types of information covered by the DPA and whether the information ‘relates to’ an ‘identifiable individual’ and is therefore ‘personal data’ regulated by the Act.

All LA's use the PSN secure service. The PSN can be used to communicate securely with GSI users. It is suitable for transferring personal data up to Impact Level 3 (RESTICTED) securely to the relevant Government Department and between PSN-connected LA's or connected agencies.

20.4 What are Impact Levels

So why do we need all this "Impact Level" stuff? For government systems there is obviously a need to make sure that information stored in them is appropriately protected. 'Appropriate' could range from open to the public information to highly secret national security information, so there needs to be a process to assess what is required in each case.

When you think about risks to information, it makes sense to think about the "What if" if the information was compromised, and the impact that it would have on the Council is a logical place to start. Central Government has grouped these into what are known as 'Impact Levels. These Impact Levels are currently defined from 0 (no impact) to 6 (severe impact).

Any member of staff using Government Connect must undergo the Baseline Personnel Security Standard (BS), which is not a formal security clearance but provides a level of assurance to the trustworthiness and integrity and probable reliability of prospective and current employees.

ABS checks involves verification of:

- Identity
- Employment history (past 3 years)
- Nationality and immigration status
- Criminal Record (unspent convictions only)

All checks will be carried out through Organisational Development.

- For the avoidance of doubt, the security rules relating to secure e-mail and information systems usage includes:

1. I acknowledge that my use of the PSN may be monitored and/or recorded for lawful purposes.

2. I agree to be responsible for any use by me of the PSN using my unique user credentials (user ID and password, access token or other mechanism as provided) and e-mail address; and,

3. will not use a colleague's credentials to access the PSN and will equally ensure that my credentials are not shared and are protected against misuse and,

4. will protect such credentials at least to the same level of secrecy as the information they may be used to access, (in particular, I will not write down or share my password other than for the purposes of placing a secured copy in a secure location at my employer's premises); and,

5. will not attempt to access any computer system that I have not been given explicit permission to access; and,

6. will not attempt to access the PSN other than from IT equipment and systems and locations which have been explicitly authorised to use for this purpose; and,

7. will not transmit information via the PSN that I know, suspect or have been advised is of a higher level of sensitivity than my PSN domain is designed to carry; and,

8. will not transmit information via the PSN that I know or suspect to be unacceptable within the context and purpose for which it is being communicated; and,

9. will not make false claims or denials relating to my use of the PSN (e.g. falsely denying that an e-mail had been sent or received); and,

10. will protect any sensitive or not protectively marked material sent, received, stored or processed by me via the PSN to the same level as I would paper copies of similar material; and,

11. will appropriately mark, using the Council's Protective Marking System Criteria; information sent via the PSN; and,

12. will not send PROTECT or RESTRICTED information over public networks such as the Internet; and,

13. will always check that the recipients of e-mail messages are correct so that potentially sensitive or PROTECT or RESTRICTED information is not accidentally released into the public domain; and,

14. will not auto-forward email from my PSN account to any other non-PSN email account; and,

15. will not forward or disclose any sensitive or PROTECT or RESTRICTED material received via the PSN unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel; and,

16. will seek to prevent inadvertent disclosure of sensitive or PROTECT or RESTRICTED information by avoiding being overlooked when working, by taking care when printing information received via PSN (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts, etc) and by
carefully checking the distribution list for any material to be transmitted; and

17. will securely store or destroy any printed material; and,

18. will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received via PSN (this will be in accordance with the computer, telephone and desk use policy - e.g. logging-off from the computer, activate a password-protected screensaver etc, so as to require a user logon for activation); and,

19. where ICT Services has implemented other measures to protect unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked requiring a user logon for reactivation), then I will not attempt to disable such protection; and,

20. will make myself familiar with the Council's security policies, procedures and any special instructions that relate to PSN; and,

21. will inform the ICT Service Desk immediately if I detect, suspect or witness an incident that may be a breach of security as stated in the ICT Security and Conduct Policy; and,

22. will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended; and,

23. will take precautions to protect all computer media and portable computers when carrying them outside my organisation's premises in accordance with the Council's ICT Security and Conduct Policy

24. will not introduce viruses, Trojan horses or other malware into the system or PSN; and,

25. will not disable anti-virus protection provided at my computer; and,

26. will comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that the Council informs me are relevant referred to in the Council's Legal Responsibilities Policy; and,

27. if I am about to leave the Council, I will inform my manager prior to departure of any important information held in my account and manage my account in accordance with the Council's ICT Security and Conduct Policy.

Appendices

Appendix A – Glossary of Terms (Definition of terms and expressions used within this document)	
All Users	Any member of staff or member that uses the Councils computer systems.
Bulletin Board	An area on the Intranet or Internet where people can share and publicise information and programs relating to their common interest.
Downloading	To transfer data, software or images from one computer to the memory of another device (e.g. smaller computer).
Electronic Systems	Fax machines; e-mail; voice mail; Internet; video conferencing; network, personal and laptop computers; mobile phones; pagers; text messaging; two-way radios; or other similar technology as may be available from time to time.
EDRM	Electronic Document and Records Management – a storage area for documents and records
End User/User	Anyone using a PC/laptop/phone.
E-mail	Message sent from an individual to one (or more) individuals or companies or bulletin boards electronically.
Executable code	A computer program that performs a task rather than just relaying a message or a set of data.
Freeware	Software that is licensed for use free of charge but with restrictions on use set by the software author(s).
Hacking	Gaining illegal access to a computer system. Abuse or security breach on any system or storage media.
IM&T	Information Management and Technology
Internet	A world wide network of computers following a recognised addressing convention so that sets of data on them are readily accessible to computer users.
Intranet	A model of the Internet, which is available only within a particular organisation – i.e. external access is not possible.
Licence	Authority from the software developer to use the software and specifying the use to which it may be put. A software licence will also

	specify the number of permitted concurrent uses of the software.
PDAs	Personal digital assistant such as a hand held personal organiser.
Personal Use	Use of Winchester City Council assets for personal (non profit) purposes. Examples may be typing a personal letter or browsing the Internet for non-work related purposes.
Personal Business	Activities relating to a private venture/business in which the employee has an interest whether financial or not.
Private Use	Use of Winchester City Council communication facilities for any calls other than emergency calls i.e. Needing to contact child minder, contact a family member.
PSN	Public Services Network (formerly GCSX).
Shareware	Software that may be used for evaluation purposes only until such times as it is registered and paid for.
Staff	Any person employed by the Council, either directly, on contract or volunteer/work experience.
USB	Universal serial bus – a standard connection method that connects an external device (such as a memory stick, joystick, camera, phone, mouse or keyboard) to a computer.
Users	Any person with access to any of the Council's systems. This will include all staff directly employed by the Council, as well as agency staff, contractors and elected Members.
Virus	Piece of software whose purpose is maliciously to alter the performance of a computer or the data that it holds. Many computer viruses are transmitted undetected alongside information or software that is wanted by the person putting it on their computer and can lie undetected until a trigger (such as a particular system date) causes it to be actioned. The effects can devastate computer installations.
World Wide Web	Graphical presentation of data on the Internet making it much more accessible and readily available to users.