Duddon Saint Peter's School

Acceptable Use Policy

Introduction

The use of electronic equipment, technology and information carries certain risks which can affect the Council in terms of legal liability, reputation and business effectiveness. Use of ICT systems must be in an ethical, professional and lawful manner. In addition, electronic communications within Government Agencies are subject to increasingly stringent standards and it is vital that the Council comply with standards such as the Government Connect Code of Connection in order to maintain vital services.

Purpose

The purpose of this policy is to establish the way ICT facilities and resources provided to staff in order to perform their duties must be used. The scope of this policy extends to all departments, employees, councillors, contractors, vendors and partner agencies who use/access ICT facilities provided or managed by Cheshire West and Chester Council, either directly or on their behalf by CoSocius Ltd.

Standards of Conduct

General Use of ICT Systems - Any information created or held on ICT systems will not be considered personal by default. It may, however, be deemed to be personal when reviewed by the Information Assurance Team when authorised to identify if it is of a personal private nature. This includes email and internet communications. Limited personal use of ICT systems is allowed provided it is in the individual's own time and the following conditions are met:-

- the sending and receipt of personal email messages is not excessive and does not interfere with work commitments of the sender.
- the email messages do not constitute misuse of email as detailed in this policy.
- the emails do not relate to any private business activities of the user or his or her relatives, friends or associates.
- Cheshire West and Chester Council's name on the email could in no way be construed as adding weight or influencing the person or organisation receiving the email.
- Staff are advised to consider marking any communication clearly as 'personal private' in the subject header. This helps ensure that your personal information is treated accordingly.
- When using ICT Systems you must make sure that you communicate in a way that supports the relevant Council policies and procedures that are specific to

your role as well as corporately adopted, including those on equalities. You should therefore make sure that you do not send/upload/post information on-line which:

- Damages the organisation's reputation or undermines public confidence in Cheshire West and Chester Council, its staff, councillors, role or services;
- Supports Political activity (other than any required in your role);
- Includes any libellous, offensive or defamatory material about any individual,
- firm, body or organisation; or could be deemed to harass, bullies or stalk another person.
- Cheshire West and Chester Council does not accept any liability for any loss or damage to any items or monies arising from use by any staff or anyone else undertaking personal financial transactions or related order issues over the Internet on any computer.

- You should not use personal electronic equipment and technology for work unless you have documented permission from your manager. If permission has been given, the standards of conduct in this policy will apply to your personal equipment when you are using it for work purposes.
- If you make an electronic comment on the internet (blogs, social media, twitter etc.) on a personal basis you must be aware that, as an employee of the Council, you are expected to comply with the standards of conduct and behaviour in this and other related policies for example: the Employee Code of Conduct, the Disciplinary Code, the Social Media Responsible Conduct Policy Staff indicating their affiliation with the Council, e.g. via an email address or other identifier, in bulletin boards, special interest groups, forums or other public offerings, in the course of their business must clearly indicate that the opinions expressed are not necessarily those of Cheshire West and Chester Council. Staff should be aware that such a statement does not exempt them from ensuring those views do not reflect negatively on the Council.
- You must not claim to represent the views of Cheshire West and Chester Council unless you have permission to do so as part of your job. Similarly, you must not try and pass off your own comments or views as being from someone else by, for example, falsifying your email address or user name or using someone else's.
- Do not send (or forward) email containing derogatory statements, subjective
- Comments likely to cause offence, gossip, hoaxes, joke or chain mail content to other people inside or outside Cheshire West and Chester Council. Staff guilty of such activity will be treated with the same possible action as if they were the originator of the content.
- The sending of unwanted messages with malicious intent can constitute harassment and would be dealt with as a disciplinary matter.
- You must not use social media, the internet, intranet, media, or social media sites to make complaints about your employment, even if areas on these sites are considered 'private'. If you want to make a complaint about any aspect of your employment with Cheshire West and Chester Council you

must use the appropriate employment procedure (e.g. Grievance, Fair Treatment at Work, Public Interest Disclosure/Whistleblowing).

- Data which involves images of people is covered by strict rules which prevent the use of sensitive data on children and vulnerable adults. You should therefore check any available guidance relating to your job and work area before using this type of data.
- You must not post images whose copyright you are not aware. Staff should not assume that because an image is available online it is copyright free and can be used without attribution or payment.
- You must make sure that any data stored and/or processed using Cheshire West and Chester Council ICT systems complies with the laws on data protection and copyright, is shared only with the intended recipient(s) and only when permission has been given or the information is already widely in the public domain.
- The Data Protection Act (1998) requires controls to be put in place to prevent
- unauthorised access to personal data. This statutory requirement strengthens the need for a high level of appropriate access controls to be developed and implemented.
- You must not email, upload or post confidential or sensitive data relating to individuals, partner organisations or any aspect of Cheshire West and Chester Council business on the internet or other public service (i.e. DropBox, Wetransfer etc) without permission from your manager .
- When sending email consider if the full email thread is required, ensure that you remove any unnecessary information from the email chain before forwarding on to others.
- When emailing multiple customers together, think about your target audience and consider if there is a need to separate your message. When emailing to groups of external email address the Blind Copy (Bcc) function should be used.
- You must maintain security of information by, for example, locking your monitor when leaving your desk regardless of the length of time and by logging off if you will not be using the system for a longer period.
- You should not leave any mobile equipment unattended unless it is absolutely necessary and if you do so you must ensure that it is secure and protected from risk of theft or use by others. Staff should not leave mobile equipment unattended on their desk for any length of period and should secure them in a drawer.

You must keep your passwords confidential (don't share them with anyone else) and comply with password security arrangements. The main requirements being:

- At least eight characters - Contain characters from three of the four categories: uppercase; lowercase; 0 through to 9; or special characters (*&^%$£"! etc.).
- Are more complex than a single dictionary word (such passwords are easier for hackers to crack).
- Do not contain two of the same characters consecutively.
- Never reveal or share your passwords to anyone and never use the 'remember password' function.

- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different Council systems.
- Do not use the same password for systems inside and outside of work.
- You should not try to use or access any part of the Council ICT systems, data or networks which you do not have permission to access or deliberately do anything which would disrupt or damage them in any way.
- You must not process or store Council information on non-authorised equipment unless approval has been given by the relevant ICT Security Team or you are using an ICT service which has been approved for use.
- All organisation or personal data stored on laptops or removable media must be encrypted including USB sticks.
- You must not download or install any software, hardware or other devices to Council ICT systems or equipment unless you have relevant authorisation to do so. All installed software must have the appropriate licenses and must be used in accordance with licence agreements.

If you manage or maintain a system it's important to prevent unauthorised access and to ensure that you maintain the confidentiality and integrity of any information, you should:-

- Consider if authorisation is required from the data owner before granting, modifying or changing access to systems or account permissions.
- Ensure that you only give access based on business need. This should be regularly reviewed and access revoked if appropriate.
- Ensure you follow any procedures that are in place to control the allocation and revoking of access rights.
- When sending, transferring, taking information offsite or sharing any data you must ensure that you follow the Council data sharing process and policies. Appropriate safeguards and controls (e.g. Encryption) must be used.

In conjunction with your position or work related responsibilities you must be aware of any legislation or mandated controls with which the Council or its partner organisations must comply with, these may include but are not limited to:

- Data Protection Act (DPA)1998
- Freedom of Information Act (FOIA)2000
- Regulations on the Reuse of Public Sector Information (RPSI) 2005
- Regulation of Investigatory Powers Act (RIPA) 2000
- Computer Misuse Act 1990
- Electronic Communications Act 2000
- Police and Criminal Evidence Act
- Copyright, Design and Patents Act 1988
- Safeguarding of Organisational Records
- Protection from Harassment Act 1997
- Sexual Offences Act 2003
- Defamation Act 1996
- PCI compliance

- PSN Code of connection
- It is a criminal offence to use a mobile device whilst driving and a conviction will attract a fixed penalty and a license endorsement. If, in connection with your employment, you are caught driving while using a mobile phone or other device you may be subject to disciplinary action and will be responsible for the payment of any fines/penalties imposed on you. Although hands free device are allowed, use should be kept to a minimum to ensure you are not distracted whilst driving.

Personal use of Council ICT systems will be permitted on a limited basis, subject to

- the standards of conduct outlined in this policy. Cheshire West and Chester Council reserves the right to restrict personal use of its ICT systems.
- Personal use of email and telephones: It is accepted that you may occasionally need to make an important personal call or to send an important personal email during working time but these should be kept to a minimum. Personal calls/emails/texts must, wherever possible, be conducted in your own time. (Note: This also applies to personal calls/emails/texts using your own personal equipment during working time).
- Personal calls/text messages on telephones: The Council reserves the right to charge for personal use of any other ICT systems provided for business use.
- Personal use of the internet: This is permitted in your own time i.e. outside normal working hours or any additional working hours approved by your line manager. You must ensure that you are recording this as non-working time in the 'flexi scheme' (Scheme of Flexible Working Hours). If you require use of the internet for personal purposes during working time you must get consent from your manager.
- Personal use of social media sites: All social media sites accessed by staff are recorded and logged. Cheshire West and Chester Council reserves the right to restrict social media access. Social Media sites must not be left running 'in the background', whilst at work. These provisions also apply to personal computers and mobile devices.

Any personal use of ICT systems must not expose security controls, systems or data to risk. You must not:

- allow non-employees (including family members) to use ICT equipment (including mobile devices, phones and tablets); or attach any personal equipment to ICT systems without the approval of the Information Assurance and Security Team.
- Store any business critical, personal or sensitive personal information in locations or systems that have not been approved.
- You must not knowingly access or try to access inappropriate internet sites, materials or downloads. This includes pornographic, illegal or other sites which would breach the Employee Code of Conduct, Disciplinary Code or equality standards and covers all Council ICT Systems or personal equipment when it is used for work purposes or in work time.

When you are using social media you must behave in accordance with the details set out in the Social Media Responsible Conduct Policy (ISP-07). Acceptable use of social media includes:-

- Being aware at all times that, while contributing to the organisation's social media activities, you are representing the Council. Staff who use social media as part of their job must adhere to the principles as set out in the Social Media Responsible Conduct Policy (ISP-07)
- When using social media sites you must not publish or post any information that you have received or have access to as a result of your employment unless you have been given permission to do so as this is confidential to your work.
- You must not use social media sites in any way that may undermine public confidence in the Council or your role within the Council, bring the organisation into disrepute, or would be discriminatory or defamatory e.g. publish or post any information including comments, jokes, illegal or prohibited images or other materials which would put the Council at risk of legal action.
- You should avoid informal personal contact with service users you work with directly or indirectly, or their carers, through social media sites (e.g. do not add them as a 'friend', 'follow' them or link with them), or using your own personal electronic equipment (e.g. email, text, calls).
- You must not use social media to harass, bully, stalk or behave in any other way that could damage your working relationships with your colleagues, members of the public or elected members.
- Be aware that personal use of social media, while not acting on behalf of Cheshire West and Chester Council, could potentially damage the organisation if an individual is recognised as being an employee. Any communications that employees make in a personal capacity through social media must therefore adhere to the principles as set out in the Social Media Guidelines.
- Whilst in work, employees are allowed limited access to social media websites from Council computers/devices or using their own equipment, in their own time and in accordance with this policy.

The Council records the use of its systems to measure system security, performance,

- whether employees are meeting the standards of conduct in this policy and for the prevention and detection of crime. This is covered in the Monitoring and Investigation Policy (ISP-09).

The Council logs all staff internet, Lync and email activity, and reserves the right to access, retrieve and delete:

- all email including in draft form, sent or received;
- all private and shared directories;
- all use of intra/internet and other communication techniques using organisational ICT systems e.g. Twitter, blogs etc; and Acceptable Use Policy
- all software on computer equipment.
- Use of the telephone, fax systems and mobile telephones will also be logged and may be in some cases be recorded.

Failure to follow the standards of conduct

- If you fail to follow the standards of conduct set out in this policy, use of ICT systems may be withdrawn from you and/or disciplinary action taken against you, up to and including dismissal.

Signed: **…….** Governor responsible

Signed: **…….** Head teacher

Date*:* *November 2015* Date of review *Autumn 2016*