Acceptable Use of ICT Policy

Contents

1 Purpose

The purpose of this policy is to set out standard working practices for the use of Information and Communication Technology (ICT) within CareTech Community Services. This includes the computing, email, Internet, telephone and fax facilities provided for staff by CareTech Community Services.

2 Policy Statement

CareTech Community Services' computing and telecommunications systems have become vital business tools and the Executive recognises that access to these facilities increases staff effectiveness and productivity. Furthermore, the introduction of these electronic systems has contributed to improving communication between staff and external contacts. However their use also poses potential security risks and can be counter-productive if used without policy guidelines.

CareTech Community Services has made a significant investment in information technology and electronic communication systems. Access to computing, email, Internet and telephone/fax facilities is provided for use by employees for the benefit of the business. These systems and any documentation or correspondence produced using these systems, are the property of CareTech Community Services.

CareTech Community Services seeks to create an appropriate balance between the protection of the employee - under the UK statutes governing human rights, personal privacy and data privacy - and the right of CareTech Community Services, under UK statute, to limit the use of its computer and telecommunications systems, and its right to monitor the uses of these systems. All users are responsible for ensuring that these CareTech Community Services facilities are used in a professional, ethical and lawful manner. In addition to this, the rules of usage detailed below govern use of the Company's computing and telecommunications systems.

This policy forms part of your terms and conditions of employment. Infringement may give rise to appropriate disciplinary action, which can include dismissal.

It is vital that you read this policy carefully. It is of critical importance that you understand and comply with these policies. If there is anything you do not understand, it is your responsibility to seek further clarification from your line manager.

3 Scope

This policy explains the steps needed to be followed by both managers and employees of CareTech Community Services in order to ensure the company applies best practice and complies with legislation.

Responsibility for reviewing this policy lies with the IT Department, in conjunction with the Company Secretary and Director of Human Resources.

This policy is subject to review on an annual basis or sooner if necessary to ensure that practices properly reflect the policy, and that the policy is feasible and effective.

4 Procedure

4.1 Personal Use of ICT

The company's computing and telecommunications systems are primarily for business use. Occasional and reasonable personal use of email, Internet access and the telephone/fax network is permitted at your manager's discretion, provided that it:

- does not interfere with the performance of your duties,
- does not interfere with the operation of the company's business or systems,
- takes place substantially out of normal working hours (e.g. at lunchtime),
- does not commit the Company to anything other than marginal costs,
- does not involve personal commercial activity (e.g. offering services or merchandise for sale),
- otherwise complies with this policy.

4.2 Privacy when using ICT

Whilst personal use of the systems is permitted, you should nevertheless have no expectation of privacy in respect of personal use of any of the company's computing and telecommunications systems. However, the company will only open files or emails that are clearly personal where it is necessary to do so for business purposes.

Remember that damaging or confidential files, email, Internet use, information or telephone/fax logs may have to be disclosed in litigation or in investigations by other authorities. You should be aware that deleting a file or email may not eliminate it from the system and consequently the company, or a third party with good reason, may still access it.

4.3 Confidentiality when using ICT

It is very important for you to understand that electronic and telecommunications systems are neither confidential nor secure and all of our systems are potentially accessible by third parties other than the intended recipient. This together with the restrictions imposed by the General Data Protection Regulation (GDPR), means that you must never reveal confidential information about anyone, without explicit permission from the 'owner' of that confidential information. This includes, but is not limited to, confidential information about clients, customers, staff, contractors, and competitors. Thus even though it may be simpler to transmit confidential information using email, the Internet or telephone/fax, do not be tempted to do so.

The company may take disciplinary and/or legal action against you for inappropriate disclosure of confidential information regarding or belonging to the company, or to an individual or company dealing with CareTech Community Services. Legal action may also be taken after the termination of your employment. Please refer to the separate CareTech Community Services Data Protection Policy for further information on dealing with personal data.

4.4 Misuse and Monitoring

The company has a duty to protect its staff from harassment and from having to work in a hostile environment. It is staff similarly have a duty not to harass, deliberately or by default, including by use of the computing, email, Internet and telephone/fax systems. You should be aware that whether any remark is harassing, discriminatory or offensive will depend on how it is received by the recipient as well as by those around you, regardless of your intention as the originator. You need to be particularly careful about the perceptions of others differing from yours; what you see as funny or clever may be received with horror and an allegation of harassment. Harassment may be a criminal offence; it is definitely a serious conduct issue and will be dealt with accordingly.

As stated earlier, all users are responsible for ensuring that CareTech Community Services computing, email, Internet and telephone/fax facilities are used in a professional and ethical manner that is consistent with this policy. Furthermore all users of the company's systems must not be engaged in the:

- Deliberate violation of any laws and regulations;
- Deliberate origination or distribution of chain letters or other 'junk' email;
- Deliberate storage, use, downloading or distribution of pirated software or data;
- Deliberate introduction and/or passing on of any virus, worm, Trojan horse, or other malicious code;
- Disabling or overloading any computer system or network, or circumvention of any system intended to protect the privacy or security of another user;
- Uploading or distribution of any software licensed to the Company, or data owned or licensed by the Company;
- Deliberate viewing, storage, downloading or distribution of pornographic or sexually explicit or otherwise offensive material.
- Viewing or otherwise communicating any illegal, racist, sexist, defamatory, obscene, pornographic or otherwise abusive or threatening messages or images. You must not send or forward jokes or other material which refer to race, sex or disability, even if they seem harmless to you.
- Sending sexual innuendoes or pestering messages.

This list is not exhaustive and may be subject to change.

Misuse of these sorts could result in liability not only for you but also the company, as anything done by any staff member in the course of employment is also treated as having been done by the employer. Violation of any of the above at any time will be treated as a disciplinary matter and may be seen as gross misconduct meriting summary dismissal.

4.5 Monitoring of ICT Systems

When using the company's computing and telecommunications facilities, employees should be aware that the company may monitor communications, regardless of whether the use is for business or personal reasons. All use of the company's facilities including personal, may be inspected, examined, reviewed, audited, disclosed or monitored by the company without notice when there is a clear business purpose, to ensure that the system is not being abused and to protect the company from potential damage or disrepute. Types of communications to which this may apply include incoming and outgoing telephone calls, faxes and emails as well as records of interaction with websites.

The company has software and systems in place that can monitor and record all computing and telecommunications facilities usage. You should be aware that our security systems are capable of recording (for each and every user) each web site visited, and each file transferred into and out of our internal networks. The company also has access to detailed telephone/fax call records.

We reserve the right to carry out monitoring activities at any time when we believe it is necessary for business purposes, both inside and outside office hours. Routine monitoring is most likely to be in the form of audits and/or spot checks. However, the company will only monitor individual employee communications where this is permitted by law and is necessary or justifiable for business reasons.

Reasons for monitoring are based on statutory provision and include:

- to establish existence of facts (e.g. to provide evidence of commercial transactions in cases of dispute);
- to ascertain compliance with regulatory practices and procedures (e.g. to ensure that employees are not in breach of any policies or procedures);
- to ensure secure and effective operations (e.g. protecting systems against viruses or hackers);
- to ensure employees are achieving the standards required (e.g. monitoring for quality control and for staff training purposes);
- to determine whether the purpose of an email is relevant to the business (e.g. checking an employee's email during his or her absence);

- to detect unauthorised or criminal use (e.g. to conduct investigations into suspected fraud).

Where there are reasonable grounds to believe that misuse has taken place or there has been a breach of the law/the company's codes of conduct, the company may conduct a more detailed investigation, potentially involving further monitoring and review of stored (but employee-deleted) data held on a server/disk/drive or other historical/archived material. Employees are reminded that deleting a file or email may not eliminate it from the system and consequently the company, or a third party with good reason, may still access it.

Gathering specific information may involve:

- examining the number and frequency of emails to and/or from a particular mail box;
- incoming/outgoing calls and faxes;
- monitoring telephone conversations;
- viewing emails sent from and received into a particular mailbox and/or stored on the server;
- viewing files stores on the server;
- the amount of time spent by a member of staff on the Internet;
- Internet sites visited and information downloaded.

In short, the nature of the facilities monitoring is not designed to extract evidence of misuse. However, where evidence of misuse becomes known as a consequence of monitoring, it will be investigated thoroughly and appropriate action taken under existing procedures.

The company will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries and archives of an individual's activities.

4.6 Using Computer Systems

You should ensure you are aware of and comply with the rules in this section, which specifically address the use of the company's internal computer systems. These rules are in addition to those already set out in previous sections that apply across the entire range of the company's computing and telecommunications facilities.

To prevent damage to CareTech Community Services systems, all computing equipment must be authorised by the IT Department before being used with CareTech Community Services existing systems. This includes but is not limited to, desktop PCs, laptops, PDAs and printers.

To prevent copyright infringements, security breaches, virus infections and other damage to CareTech Community Services systems, all software must be authorised by the IT Department before being installed or used with CareTech Community Services systems. This includes but is not limited to, store-bought and downloaded programs, screen savers, logos, games, video and music files.

To make best use of IT resources, staff should regularly review the contents of their files and mailboxes. Unwanted files and emails should be deleted.

IT equipment is expensive and fragile. Staff must ensure they take all reasonable precautions to protect it from damage and theft.

Notify the IT department of any IT related problems as soon as you can. This particularly includes information regarding staff that are starting or leaving, as well as any temporary workers that require access to the IT systems.

4.7 Security of Computer Systems

User IDs and passwords help maintain individual accountability for computing system resource usage. Any staff member who obtains a password or ID must keep that password confidential. Do not write your password down and do not disclose it to anyone. If you think someone else knows your password you should change it immediately. If you need to give a colleague access to your work it can be done without disclosing your password. Contact the IT Helpline for advice.

To prevent accidental disclosure of information your workstation will lock automatically after a set period, however you should always lock your workstation when you are away from it. You can lock your workstation by pressing CTRL-ALT-DEL followed by ENTER. You can unlock your workstation by pressing CTRL-ALT-DEL and entering your password.

4.8 Data Handling

All CareTech Community Services staff who hold personal data (on paper or electronically) must keep that data secure. Personal data is defined as the combination of data items (held by the organisation, not necessarily by an individual staff member) that identifies an individual (employee, customer, and supplier/contractor) and provides personal information about them, their families or circumstances the compromise of which could cause distress or harm to that individual. This includes names, contact details, gender, dates of birth, bank account details, health details, academic records, skills or abilities, and behavioural or attendance records.

With regard to personal data stored on computers especially laptops and removable portable devices or media including flash drives, memory sticks and pens, thumb drives, removable hard drives, CDs, DVDs, PDAs, Blackberry's, smartphones; it is strongly advised that any personal data stored on laptops is either removed or , as a minimum is password protected. Similarly no other storage medium (whether it be owned by CareTech Community Services or not) is to contain personal data about staff or service users unless that medium is similarly protected. Failure to comply with this directive will compromise CareTech Community Services' obligations under the General Data Protection Regulation (GDPR) and will result in disciplinary actions against the offender.

4.9 Email Use

You should ensure you are aware of and comply with the rules in this section, which specifically address the use of email within the company. These are in addition to those already set out in sections that apply across the entire range of the company's computing and telecommunications facilities.

The most common method of virus transmission into computing systems is via email. You should always be suspicious of attachments that arrive unexpectedly even if they appear to come from someone you know. If in doubt, don't open the message and contact the IT Helpline immediately.

You should be aware that email messages carry the same weight in court as printed letters on company letterhead. Thus, ill-considered messages could have serious repercussions. For example, you may be held to account for making defamatory remarks via email. A defamatory statement is one that tends to damage the reputation of another individual or organisation. You must not participate in office gossip and/or spreading rumours over the email system about clients, customers, staff, contractors, competitors – in short, anyone. Even if it may seem innocent to you, it may give rise to liability for defamation by both you and the company.

The company by its very nature gives a great deal of advice to a wide range of people – this advice is obviously given through its staff. You will know whether or not it is part of your duties to give advice via email and the extent of your authority to do so. If you are acting within the normal course of your duties and your expertise, and you act in good faith without malice or capriciousness, then you will be protected even if your advice proves to be wrong. However, if you act outside your competence or outside your authority then again you may be liable for any harmful consequences of your actions. If you are asked to give advice in email, and you are unsure whether or not you are competent to give it, then don't - at least not without seeking advice yourself. Never give gratuitous advice on an area that is not within your expertise; you may be liable to any third party who relies upon it to his/her detriment, not just the person to whom you addressed it.

Do not enter into contractual commitments by email without legal advice. Email is capable of forming or varying a contract in just the same way as a written communication. Because of the perceived informality of email, there is the danger of contracts being inadvertently formed by employees, to which the company is then bound. You must comply with the following rules before entering into contracts by email:

- You must obtain authorisation before negotiating contracts by email
- You must take advice from your manager before entering into contractual commitments
- Managers should always seek advice from the Company Secretary
- You must include the statement "subject to contract" in all emails if you conduct contractual negotiations via email until such time as it is intended that a binding contract should come into existence
- You must be satisfied of the legal identity of the other contracting party before entering into a binding contract via email

4.10 Email Etiquette

In addition to the above rules, the following guidelines should be followed when using the email system:

- Always maintain a professional image. Ensure the style, tone and content of emails is appropriate
- Do not use email for urgent messages. Use the telephone. It should be noted that the delivery and integrity of email cannot be guaranteed
- Respond to emails in a timely and professional manner
- Always acknowledge receipt of emails requiring responses even if you cannot reply fully straightaway
- Send emails only to those recipients/groups for whom the message is intended
- Ensure the subject matter is clearly indicated in the heading
- Try to use plain text in emails. Fonts, underline, colour, graphics and tables not only add to the message size, slow systems down and may adversely affect delivery times but may also be lost in external emails
- Limit the number and size of your file attachments as they result in increased traffic around the company's network and may incur the displeasure of external correspondents if they must pay to be connected whilst downloading the resulting large email message
- Avoid sending excessive numbers of trivial messages, jokes, gossip or adverts by email
- Know that the company reserves the right to limit absolute message sizes allowed into or out of its email network
- Identify your contact details in emails
- Re-read and spell check messages prior to sending to ensure accuracy and clarity

- Read and delete emails regularly
- Remember to activate your Out of Office Assistant when you are away for more than a day – this way others will know you are not actively reading your email
- Email messages can be impersonal and/or misinterpreted so when sending an email consider whether it is the most effective method of communicating in that situation

4.11 Internet Use

You should ensure you are aware of and comply with the rules in this section, which specifically address the use of the company's Internet facilities. These policies are in addition to those already set out in sections that apply across the entire range of the company's computing and telecommunications systems.

The company encourages authorised staff to access the Internet during working hours, when direct work-related benefits can result. However, there are limits to personal use of the Internet, which are set out elsewhere in this policy. You should note:

- Different access for different types of personnel may be given;
- The company reserves the right to block access to certain Internet sites;
- Internet sites that are cost related or have cost implications in their terms of access must not be subscribed to without the prior authority of the relevant budget holder;
- Without prior approval from the IT Department, you may not download software or files from the Internet for use on the Company's systems;
- Any such software or files that are approved for download via the Internet become the property of the company and may be used only in ways that are stipulated by their licences or copyrights and in a manner consistent not only with this policy but with the requirements outlined by the IT Department;
- Excessive personal use of the Internet during or outside business hours is not allowed;
- Downloading entertainment software or games, or playing games against opponents over the Internet or Intranet at any time is forbidden.

Do not download, store, reproduce or distribute documents, pictures, logos, music or works of others without the owner's permission as this may infringe copyright laws. If you download articles and other materials from the Internet, you must remember that you need permission from the author before using such information for business purposes. The dissemination of copyrighted information is a disciplinary offence which may result in disciplinary action being taken against you including in serious cases dismissal. If in doubt, speak to your manager about whether a particular work is copyrighted. Managers may seek guidance from the Company Secretary if necessary.

5 Summary of Acceptable Use of ICT

CareTech Community Services provides computer and telecommunications systems for use by employees in support of its activities. All users are responsible for ensuring that these systems are used in a professional, ethical and lawful manner. Therefore, it is important to define acceptable use principles to protect the staff, the company and the information itself. This document is intended as a summary of your responsibilities as an employee, as defined in CareTech Community Services' 'Acceptable use of ICT Policy and Procedure' and forms part of your contractual Terms & Conditions.

IMPORTANT: All uses of CareTech Community Services computing and telecommunications systems may be monitored, as circumstances warrant. Infringement of this policy may give rise to appropriate disciplinary measures. If you are not certain you fully understand and can comply with this policy you should seek further clarification from your Line Manager.

5.1 Limit personal use

At your manager's discretion, occasional personal use of email, internet, telephone and fax systems is permitted as long as it does not interfere with staff productivity or responsibilities, and does not incur costs.

5.2 Manage your virtual space

Virtual space, like office space, is finite and expensive. Delete files or email messages you do not need anymore. Avoid keeping multiple copies of files unless absolutely necessary.

5.3 Only use software & hardware authorised by the IT Department

To prevent copyright infringements and damage to CareTech Community Services systems, all computing equipment (including laptops, PDAs and printers) must be authorised by the IT department before being used with CareTech Community Services systems. Similarly, all software (including logos, games and video/music files) must also be authorised by the IT department before being used with CareTech Community Services systems.

5.4 Help your colleagues

Activate your Out of Office Assistant when you are away – this way others will know you are not actively reading your email.

5.5 Help the IT department to help you

Notify the IT department of any IT related matters as soon as you can. This includes information regarding staff that are starting or leaving, as well as any temporary workers that require access to the IT systems.

5.6 IT Security

Keep your password secret. Do not write it down and do not give it to anyone – even someone from the IT department. If you think someone else knows your password you should change it immediately. If you need to give a colleague access to your work please contact the IT Helpline for advice. Change your password every 3 months. Do not use a password that you have used before, and do not use passwords that are obvious or easy to guess.

Lock your workstation when you are away from it. Lock your workstation by pressing CTRL-ALT-DEL followed by ENTER. Keep IT safe, IT equipment is expensive and fragile. Make sure you take all reasonable precautions to protect it from damage and theft.

5.7 Email & Internet

Never send confidential information via email. Email is neither private nor secure. If you need to email confidential information contact the IT Helpline for advice. Email can be legally binding. Never put anything in email that you would not be prepared to put on letterhead and sign. In court an email is the same as a printed document. If you are unsure ask your Line Manager for advice.

Always be suspicious of attachments that arrive via email. This is especially true of anything you do not expect to receive, even if it appears to come from a well-known source. If in doubt, don't open it. Contact the IT Helpline for advice. Use the Internet and email facilities appropriately. Do not view, download, save or transmit offensive, pornographic, or any other inappropriate material. Similarly, do not use copyrighted material without the owner's permission. Inappropriate use may lead to summary dismissal as well as being reported to the police. If you have any questions regarding this document please contact the IT department on it.support@caretech-uk.com

6 Revision History

Date of next review: March 2018
Date of release: March 2016