ICT systems Policy

Contents

ICT systems Policy

Application of this policy:

This policy covers the use of computer hardware and software, email, the internet, telephones, mobile phones and fax facilities (the "ICT Systems").

Acceptable standards of use:

We are concerned to uphold our good name and reputation and to offer proper protection from inappropriate use of the ICT Systems to all employees, contractors, students and suppliers.

All use of the ICT Systems must always meet the Acceptable Standards of Use set out in this policy. As with all aspects of this policy, failure to follow the policy will result in disciplinary action and, in appropriate cases, dismissal.

The following use of any of (or any part of) the ICT Systems provided by us is totally unacceptable:

- Accessing, viewing, creating, storing or transmitting (or any attempt to do so) material which is designed or likely to cause annoyance, offence, inconvenience or needless anxiety (even if it does not come to the attention of the person(s) whom it concerns).
- Accessing, viewing, creating, storing or transmitting (or any attempt to do so) any offensive, obscene, pornographic or otherwise indecent images, data or other material or any data capable of being resolved into obscene or indecent images or material.
- Creating, storing or transmitting dishonest, misleading or defamatory material.
- Accessing, viewing, creating, storing or transmitting material which contains inappropriate references (without limitation) to religion, race, ethnic origin, nationality, sexual preference and/or gender. Remember: what constitutes offensive material varies from person to person - if in doubt do not send it, create, store it or save it.
- Infringing copyright or other intellectual property rights. This can be a complicated area; information can be in the public domain e.g. published on the internet but still be subject to copyright and not freely reproducible - if in any doubt then please seek assistance from ICT before using any such material.
- Advertising services or products other than those of the business without proper advanced authorisation.
- Deliberate unauthorised access to (or attempts to access) facilities which may be accessible via our network.
- Corrupting or destroying (or otherwise moving, concealing or restricting access to) other users' or business data (or any attempt to do so).
- Violating the privacy or disrupting the work of other users (including by sending unnecessary messages) (or any attempt to do so).

- The unauthorised use of system facilities to mask your identity or permit one user to masquerade as another or as the system operators (or any attempt to do so).

- Negligently or deliberately introducing a virus, Trojan or worm program (or any other such program or material designed to cause damage to any system) to any system (even if the effect is not destructive).

- Any action which amounts to the harassment of another user.

- Gambling.

- Sending, forwarding or disseminating of chain or junk emails/faxes or inappropriately large emails or files or indeed in the sending, forwarding or disseminating of multiples of emails/faxes where this is not required for the purposes of the business (e.g. marketing, announcements to employees etc.).

PERSONAL USE:

The ICT Systems are provided by us to meet business needs.

Personal use of our office address and stationery are not permitted. Personal use of email, the Internet, business telephone and mobile phone and fax, are allowed so long as use is kept within the limits set out in this policy.

Extent of Use:

The IT Equipment and/or the communications system should never be used for any purposes other than those of The John Graham Centre (JGC) nor should they be used for personal gain.

You may only use telephones for emergency personal telephone calls if absolutely necessary, but this must be restricted to the minimum.

VIRUSES AND SYSTEM PROTECTION:

All use of the computer hardware software, the Internet, email and mobile phones must be in accordance with this Virus and System Policy (set out below).

We rely increasingly upon our computer hardware, software, email, the Internet and mobile phones in our business operations as a means to achieve competitive advantage. More and more systems are being deployed on Personal Computers (PC, desktop, laptop and

handheld devices) and Local Area Networks (LANS). These platforms can be vulnerable to increasingly sophisticated computer viruses unless adequate security measures are observed.

Virus awareness:

It is the responsibility of all employees to be aware of the potentially damaging risks posed by viruses and other unwanted software and materials.

You should always be alert to the risk of receiving emails, software or data (on disk or otherwise) potentially containing viruses, Trojans, worms or other harmful or unwanted material. As a general guide employees should:

- Ensure that any software or data to be installed on our computer hardware is screened through the approved antivirus software prior to being installed or loaded onto our computers. This must be done each time software or data is installed or loaded regardless of the source of the data or information. Failure to screen may be considered a disciplinary offence.

- Be wary of emails and electronic material from an unusual or unknown source. In the case of any doubt you should delete the email and also delete the email from any Deleted Items folder.

- If you believe you may have received a virus in an email or attachment that you need to keep then you should immediately contact the centre manager to seek urgent assistance (do not open the email). If you receive an email containing a virus that you do not need you should delete the email and remove it from your deleted items and then inform the centre manager of the sender of the email.

Computer software & Hardware:

General:

All computers are loaded with specific software at the time of installation to perform specific tasks. The software is updated or replaced periodically to meet business needs.

Obtaining software:

All software purchases must be approved by the manager in advance. This will ensure that only software which meets business needs, and which is compatible with hardware and other software is installed. It also ensures that all software is licensed, inventoried and loaded in a standard fashion.

Installing software:

Usually IT will install software. No software may be installed without the prior approval of the manager, however, if the manager allows you to install software, you must follow any instructions precisely. This applies however software is installed (including by Internet download and whether it is provided free of charge or not).

Using software:

You must only use software for the purposes for which it has been provided and within the terms of the licence for that software. You must never use any software which has not been approved in advance by the manager and should inform the manager upon becoming aware that any unapproved software is installed on any of the IT equipment or the communication systems.

Software registration:

All software on our computer equipment will be registered to us. We purchase and license the use of software for business purposes and in most cases do not own copyright to it.

You must not reproduce any software or use it in a way that lies outside the terms of the licence. All licence documentation must be returned to the Managers.

Protecting hardware and software:

It is your responsibility to protect from damage hardware, software and data which you are using, or which has been made available for your use.

All of the IT systems are and remain our property and should always be treated with suitable care to avoid loss or damage to all or any part of them.

Passwords/logging off:

Passwords must not be written down or disclosed to anyone else without proper authority. Passwords should be at least eight characters long and include at least three different types of character (i.e. upper and lower case, numbers and symbols). Users should not use names; car registration numbers or dates of birth and passwords must be changed every month.

You are responsible for any activity which originates from your PC and for all the information stored in your personal file space. As a result, and as a security measure you should password protect your screen saver and ensure that the screen saver is activated whenever you leave your PC for short periods of time. You should also always log off from your computer whenever you are away from it for any substantial period to prevent unauthorised access or misuse.

Installing/uninstalling hardware:

You should never install hardware or otherwise attach or connect (physically or by infrared or other remote connection) any device (including a mobile phone, laptop computer or other hand held device) to any of the IT systems unless you have the prior authorisation from the manager to do so. By the same token, you should never uninstall or remove any hardware without prior permission.

Email - Acceptable Standards of Use:

Please remember that all use of email whether internal or external should always comply with the Acceptable Standards of Use noted above and the other terms of this policy. Staff must ensure when emailing data protection must be taken into consideration and maintain privacy at all time.

Virus protection:

Please also note that all use of email must be in accordance with our Virus and System Protection Policy.

Alternatives:

Email when used properly is an extremely effective form of business communication both internally and externally. However, email is a very impersonal communications medium. It can be easy to cause offence. You should always consider before sending an email or continuing an exchange of emails whether or not it is or remains the appropriate

communication medium. Consideration should be given to whether a face-to-face meeting or telephone discussion may be more appropriate.

Style:

Email is an informal and almost instantaneous form of communication. As a result, it is easy to overlook the normal protocols that you would apply when for example sending a letter.
As a guide, you should:

- Remember to use a greeting and sign off - a personal touch makes email more pleasant.
- Don't forget to use please and thank you as you would in normal speech.
- It is tempting to use character styles to make a point more strongly. However, many users regard some of these techniques as rude or annoying.
- Remember to check all emails for spelling, punctuation, grammar and layout before you send it.
- Insert the address of the recipient after drafting and checking an email to prevent inadvertent transmission.
- Use an appropriate subject heading.
- Do not write anything that you would not write in a letter.

Content:

You must not indicate in any private email that you are acting on behalf of the business.

You must not indicate in any email that any information you give is an official business document and in addition you must not represent your opinions as those of the business unless you are authorised to make such statements.

You will not make any suggestion about any facet of the business or its services or make any suggestion that you have authority to enter into a contract unless you have specific authority to do so.

Particular care should be taken with attachments to outgoing email. Before sending you must double check that you have the correct attachment by opening and checking each document attached to the outgoing email.

Email may only be sent externally by those who have authority to sign their outgoing post. Any person who does not fall into this category should first gain authorisation for the email to be sent.

If you receive an email which contains offensive or obscene material, you should produce a paper copy to the Manager Angela Cook or a supervisor as soon as possible. It must then be deleted from your Inbox and your Deleted Items box immediately.

Overuse/proliferation:

Always consider to whom a message is relevant before you send it. This includes cc addresses as well.

Attempt to target emails to appropriate recipients only; this will avoid disruption to people to whom the message is not relevant.

Only use the "Reply to All" or "Reply to sender and all recipients" (or such similar option) when you intend your reply to be seen by the sender and all other recipients.

Only use the "Reply to sender (and all recipients) with original message" (or such similar option) when it is appropriate for the recipients to see the message history.

Prioritise messages honestly and accurately.

Use appropriate "Subject" headings where possible to assist the recipient(s) in prioritising the message. As a general guide, some suggested priority categories are:

Urgent	**Normal**	**Low**
Urgent information (for all recipients)	Job specific material	General Information
Essential material for meetings	Specific messages/replies	Course availability
Immediate response required		Social events Press releases

Protecting confidentiality/security:

Confidential Information should not normally be sent by email without security measures. This could include password protection of files, prior arrangements with recipients to ensure safe and confidential receipt. If you are in any doubt as to the confidential nature of any material, then check with the Management before sending any messages containing that material. It is your responsibility to keep confidential all business information which you publish or use on the system.

You should always ensure that the addresses(es) of recipients are accurate and up to date before sending an email to avoid inadvertent disclosure of information.

All outgoing external email will automatically have added to it a confidentiality notice.

You should ensure that access to your email is restricted to you and anyone who reasonably requires access in the course of your work. You should not register your email address with any outside body without the prior consent of the manager in order to avoid the risk of system overload from junk or unwanted emails.

The Internet:

Acceptable Standards of Use:
As mentioned above all use of the Internet should always comply with the Acceptable Standards of Use and the other terms of this policy.

Virus protection:
All of use of the Internet must be in accordance with our Virus and System Protection Rules.

Internet use/access:

It is possible to access the Internet from our network. Access is granted for business use only to some users. The facility to access the Internet must be authorised beforehand by the manager or a supervisor.

All software used to access the Internet or downloaded from it must be used and/or downloaded/installed in accordance with the rules set out in this policy.

The Internet may only be accessed:

- by connection to our Internet Gateway which is only possible from a computer connected directly to our network.
- by connection direct to an Internet service provider from a computer that is never connected to our network.

Care should be taken to disconnect once the information sought is obtained.

Hyperlinks and web site addresses (URLS):

You should take care when entering web site addresses in order to ensure that you do not inadvertently access sites which are not in accordance with our Acceptable Standards of Use. By the same token, Hyperlinks are often difficult to control and should be used with reasonable caution. Should any inappropriate site(s) be accessed please immediately report the fact to the Manager in order that access to the site can be blocked.

Telephone, Fax machines & Mobile phones:

Voicemail:

Our voicemail system is designed and intended to form an integral part of the IT facilities available to employees. Voicemail use must always be in accordance with our Acceptable Standards of Use.

Fax machines:

Fax machines should be used in accordance with our Acceptable Standards of Use.
Users should check that the number to which the fax is sent is correct.
If the information to be sent is private and confidential users should check by phone that the recipient is waiting to collect it (unless users have already established that the fax is in a secure and private location).

Mobile phones:

All use of mobile phones must be in accordance with our Acceptable Standards of Use and our Virus Protection and System Protection Rules.
(Please see below)

REMOTE USERS:

Remote access users must be particularly careful not to allow a laptop computer to be accessed by non-authorised persons. If, for any reason, you believe that this has

happened, or in the event that your laptop is lost or stolen, you must inform the manager immediately.

Laptops must always be locked in a secure area when not in use and should never be left unattended in vehicles. Laptops should always be carried in their protective cases. You are responsible for ensuring protection from damage.

Monitoring Communication systems usage:

Access to all communication systems:
You should be aware that:

- We retain the right to access all and any information stored on or in any of the IT equipment or communication systems. As a result, employees, should be aware that no information stored on or in IT equipment or the communication systems is private.
- In addition, we monitor your use of email and the Internet in order to ensure compliance with the terms of this policy and for other legitimate business purposes.

Mobile Phone Use:

If you are provided with a mobile telephone this is to be used for work telephone calls only. If the telephone is used for private telephone calls, we will require you to reimburse the cost of these calls. You should take care of the telephone and ensure that it is secure at all times. In the event that the telephone is lost or stolen you should notify the manager or a senior immediately to report the loss or theft. In the absence of the managers/ seniors, you should take all reasonable steps to report the matter to a member of the office team so that arrangements can be made to disconnect the telephone.

Mobile phones should never be used for personal calls directly outside our buildings or premises or within reception or other places accessible by our students, contractors or suppliers.

Your company or private mobile phones should not be used to send or receive private calls or text messages during working hours except in a genuine emergency.

We are committed to continuously improving health and safety for our employees and believe that using a mobile phone when driving or operating machinery is dangerous.

It is known that using a handheld mobile phone, or other computerised or communication device, whilst driving increases the risk of accident because the driver is distracted from managing their vehicle safely. This includes talking via a mobile phone as well as sending text messages and making or answering calls.

Therefore, you should not make or receive calls on your company or personal mobile phone (or other device) whilst driving on JGC business (whether in your own or company vehicle) except when it is parked and stationary.

JGC accepts no liability in the event of an accident occurring whilst driving or operating machinery and using a mobile phone (or any hand-held communication or computerised device). Anyone who is found to have used such phones and devises whilst driving on JGC business or operating machinery, will be liable to disciplinary action.

Appropriate messages should be recorded on your company mobile phone inviting callers to leave a brief message and phone number and detailing:

- That their call will be returned as soon as possible
- Another contact number to call in case of urgency.

Review Date:16.02.23