ICT POLICY

ORIGINATOR: Gary Stone
SLT LINK: Stuart Williams

July 2020

Contents

1. POLICY STATEMENT

1.1 Within this policy 'we' and 'us' means the Federation.

1.2 By following this policy we will help ensure that our ICT facilities are used:

- legally;
- securely;
- without undermining us;
- effectively;
- in a spirit of co-operation, trust and consideration for others;

1.3 The policy relates to all ICT facilities and services provided by us, although special emphasis is placed on email and the internet. All employees, and any other users of our IT, are expected to adhere to the policy.

1.4 The ICT equipment covered by this policy includes all hardware and software systems including, but not limited to, desktop machines, laptops, mobile phones, tablets, email and social media. ICT for the purposes of this policy will also include personal ICT devices when connected to the Federation network.

2. DISCIPLINARY MEASURES

2.1 Deliberate and serious breach of the policy statements in this section may lead us to take disciplinary measures in accordance with our Disciplinary Policy. We accept that ICT, especially the internet and email system, is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the organisation.

2.2 In addition, all of our phones, internet and email related resources are provided for business purposes. Therefore, we maintain the right to monitor the volume of internet and network traffic, together with the email systems. The specific content of any transactions will only be monitored with the authorisation of the Executive Principal, following reasonable suspicion of improper use.

3. SECURITY

3.1 As a user of our equipment and services, you are responsible for your activity.

3.2 Do not disclose personal system passwords or other security details to other employees or external agents, and do not use anyone else's log-in; this compromises our security. If someone else gets to know your password, ensure that you change it immediately or get a member of the IT Team to help you.

3.3 If you intend to leave your PC or workstation unattended for any reason, you should lock the screen to prevent unauthorised access. If you fail to do this, you will be responsible for any misuse of it while you are away – you are responsible for the actions someone else takes whilst using your account. Logging off is especially important where members of the public have access to the screen in your absence.

3.4 Any pen drives or other storage devices which you use on our network should be secure and only those that are our property should be used. For more detail, please see the section on Removable Media.

3.5 Do not attempt to gain unauthorised access to information or facilities. The Computer Misuse Act 1990 makes it a criminal offence to obtain unauthorised access to any computer (including workstations and PCs) or to modify its contents. If you do not have access to information or resources you feel you need, contact your line manager.

4. USE OF EMAIL

4.1 When to use email:

4.1.1 Use email in preference to paper to reach people quickly (saving time on photocopying / distribution) and to help reduce paper use.

4.1.2 Use the phone for urgent messages (email is a good back-up in such instances). Use of email by our employees is permitted and encouraged where such use supports the goals and objectives of the organisation.

4.1.3 However, we have a policy for the use of email whereby employees and volunteers must ensure that they:

- comply with current legislation;
- use email in an acceptable way;
- do not create unnecessary business risk to us by their misuse of the internet.

4.2 Unacceptable behaviour

4.2.1 Sending confidential information to external locations without appropriate safeguards in place. See point 5 of this document for more details.

4.2.2 Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal.

4.2.3 Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment or bullying.

4.2.4 Using copyrighted information in a way that violates the copyright.

4.2.5 Breaking into our or another organisation's system, or unauthorised use of a password / mailbox.

4.2.6 Broadcasting unsolicited personal views on social, political, religious or other non-business related matters.

4.2.7 Transmitting unsolicited commercial or advertising material.

4.2.8 Undertaking deliberate activities that waste employees' effort or network resources.

4.2.9 Deliberately or recklessly introducing any form of computer virus or malware into the corporate network.

4.3 Confidentiality

4.3.1 Always exercise caution when committing confidential information to email since the confidentiality of such material cannot be guaranteed. We reserve the right to monitor electronic communications in accordance with applicable laws and policies. The right to monitor communications includes messages sent or received by system users (employees and temporary employees) within and outside the system, as well as deleted messages. Further information can be found within this policy.

4.3.2 General points on email use:

4.3.2.1. When publishing or transmitting information externally, be aware that you are representing us and could be seen as speaking on our behalf. Make it clear when opinions are personal. If in doubt, consult your line manager.

4.3.2.2. Check your inbox at regular intervals during the working day. Keep your inbox fairly empty so that it just contains items requiring your action. Try to decide what to do with each email as you read it (e.g. delete it, reply to it, save the whole email in a folder, or extract just the useful information and save it somewhere logical).

4.3.2.3. Keep electronic files of electronic correspondence, only retaining what you need to. Do not print it off and keep paper files unless absolutely necessary.

4.3.2.4. Treat others with respect and in a way in which you would expect to be treated yourself (e.g. do not send unconstructive feedback, argue, or invite colleagues to make public their displeasure at the actions / decisions of a colleague).

4.3.2.5. Do not forward emails warning about viruses. Instead contact a member of the IT team and make them aware of the email.

4.3.2.6. Do not open an email unless you have a reasonably good expectation of what it contains, and do not download files unless they are from a trusted source. For example, do open a report.doc file from a colleague you know but do not open explore.zip sent from an address you have never heard of, however tempting. Alert the IT team if you are sent anything like this unexpectedly; this is one of the most effective means of protecting us against email virus attacks.

4.4 Email signatures

4.4.1 Keep these short and follow our Brand Guidelines, they should include your full name and job title, usual working days and hours and the main reception contact telephone number.

5. USE OF THE INTERNET

5.1 Use of the internet by employees is permitted and encouraged where such use supports our goals and objectives.

5.2 However, when using the internet, employees must ensure that they:

- comply with current legislation;
- use the internet in an acceptable way;
- do not create unnecessary business risk to the organisation by their misuse of the internet.

5.3 Unacceptable behaviour

5.3.1 In particular, the following is deemed unacceptable use or behaviour by employees, however, this list is non-exhaustive:

- Visiting internet sites that contain obscene, hateful, pornographic or other illegal material.
- Using the computer to perpetrate any form of fraud, or software, film or music piracy.
- Using the internet to send offensive or harassing material to other users.
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence.
- Hacking into unauthorised areas.
- Creating or transmitting defamatory material.
- Undertaking deliberate activities that waste employees' effort or network resources.
- Deliberately or recklessly introducing any form of computer virus into our network.
- Sharing/posting confidential information to an unauthorised website.

5.4 Chat rooms / instant messaging (IM)

5.4.1 The use of chat rooms and instant messaging is permitted for business use only. This use must have been agreed with your line manager. This applies to any forms of communication.

5.5 Webmail

5.5.1 The use of webmail (e.g. Hotmail, MSN, Gmail) is not permitted in the organisation unless previously agreed with your line manager. All of our business should be from our email accounts only. Under no circumstances should school emails be forwarded to personal accounts, unless it is your own personal data regarding your employment.

5.6 Obscenities / pornography

5.6.1 Do not write, publish, look for, bookmark, access or download material that might be regarded as obscene or pornographic.

5.7 Copyright

5.7.1 Take care to use software legally and in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges.

5.7.2 Be aware of copyright law when using content you have found on other organisations' websites. The law is the same as it is for printed materials.

6. CONFIDENTIALITY

6.1 If you are dealing with personal, sensitive and / or confidential information, then you must ensure that extra care is taken to protect the information.

6.2 If sending personal, sensitive and / or confidential information via email, then the following protocols should be used. If there is any doubt as to the information being sent or the appropriate level of protection required, please check with the Network Manager.

- Personal, sensitive and / or confidential information should be contained in an attachment;
- In appropriate cases the attachment should be encrypted, and / or password protected;
- Any password or key must be sent separately;
- Before sending the email, verify the recipient by checking the address, and if appropriate, telephoning the recipient to check and inform them that the email will be sent;
- Do not refer to the information in the subject of the email.

7. OUR NETWORK

7.1 Keep master copies of important data on our network or authorised cloud server and not solely on your PC's local C: drive or portable disks. Not storing data in this way means it will not be backed up and is therefore at risk.

7.2 Ask for advice from the Network Manager if you need to store, transmit or handle large quantities of data, particularly images or audio and video. These large files use up disk space very quickly and can bring the network to a standstill.

7.3 Be considerate about storing personal, non-Federation files on our network.

7.4 Do not copy files that are accessible centrally into your personal directory unless you have good reason (i.e. you intend to amend them or you need to reference them and the central copies are to be changed or deleted) since this uses up disk space unnecessarily.

8. REMOVABLE MEDIA

8.1 If storing or transferring personal, sensitive, confidential or classified information using Removable Media you must first contact The Data Protection Officer for permission, and also:

- Always consider if an alternative solution already exists.
- Only use recommended removable media.
- Encrypt and password protect.
- Store all removable media securely.
- Removable media must be disposed of securely by the Network Manager.

9. PERSONAL USE OF ICT FACILITIES: SOCIAL MEDIA

9.1 For the purposes of this policy, social media websites are web-based and mobile technologies which allow parties to communicate instantly with each other or to share data in a public forum. They include but are not limited to; websites such as Facebook, Instagram, Snapchat, TikTok, Twitter, Google and LinkedIn. They also cover blogs and image sharing websites such as YouTube and Flickr. This is not an exhaustive list and you should be aware that this is a constantly changing area.

9.2 Use of Social Media at work

9.2.1 Employees and volunteers are permitted to make reasonable and appropriate use of social media websites from our IT equipment. You should ensure that usage is not excessive and does not interfere with work duties. Use should be restricted to only your non-working hours, unless this forms part of your work responsibilities.

9.2.2 Access to particular social media websites may be withdrawn in the case of misuse.

9.2.3 Inappropriate comments on social media websites can cause damage to the reputation of the organisation if a person is recognised as being an employee. It is, therefore, imperative that you are respectful of the organisation's service as a whole including clients, colleagues, partners and competitors.

9.2.4 Employees should not give the impression that they are representing, giving opinions or otherwise making statements on behalf of the Federation unless appropriately authorised to do so. Personal opinions must be acknowledged as such, and should not be represented in any way that might make them appear to be those of the organisation. If in doubt, an explicit disclaimer should be included, for example: 'These statements and opinions are my own and not those of the Federation.'

9.2.5 Any communications that employees (or volunteers) make in a personal capacity must not:

- bring us into disrepute, for example by criticising clients, colleagues or partner organisations;
- breach our policy on client confidentiality or any other relevant policy;
- breach copyright, for example, by using someone else's images or written content without permission;
- do anything which might be viewed as discriminatory against, or harassment towards, any individual, for example, by making offensive or derogatory comments relating to: age, disability, gender reassignment, race, religion or belief, sex, or sexual orientation;
- use social media to bully another individual;
- post images that are discriminatory or offensive (or links to such content).

9.2.6 We maintain the right to monitor usage where there is suspicion of improper use.

9.3 Other personal use

9.3.1 Use of facilities for leisure or personal purposes (e.g. sending and receiving personal email, personal phone calls, playing computer games and browsing the internet) is permitted so long as such use does not:

- incur specific expenditure for us.
- impact on the performance of your job or role (this is a matter between each member of employees and their line manager);
- break the law;
- bring us into disrepute;
- detrimentally affect the network performance by using large amounts of bandwidth (for instance by downloading / streaming of music or videos);
- impact on the availability of resources needed (physical or network) for business use.

9.3.2 Any information contained within our network is for use by the employee for the duration of their period of work and should not be used in any way other than for proper business purposes, or transferred into any other format (e.g. loaded onto a memory stick / pen drive), unless necessary for business use, and with prior agreement of the Executive Principal.

10. PORTABLE AND MOBILE ICT EQUIPMENT

10.1 This section covers items such as laptops, mobile devices such as phones or watches and removable data storage devices. Please refer to the section on Removable Media when considering storing or transferring personal or sensitive data.

10.2 Use of any portable and mobile ICT equipment must be authorised by the Executive Principal before use.

10.3 All activities carried out on our systems and hardware will be monitored in accordance with the general policy.

10.4 Employees must ensure that all data belonging to us is stored on our network and not kept solely on a laptop. Any equipment where personal data is likely to be stored must be encrypted.

10.5 Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of the car before starting your journey.

10.6 Synchronise all locally stored data, including diary entries, with the central organisation network or approved cloud based server on a frequent basis.

10.7 Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.

10.8 The installation of any applications or software packages must be authorised by the Network Manager, fully licensed and only carried out by the Network Manager.

10.9 In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.

10.10 Portable equipment must be transported in a protective case if one is supplied.

11. REMOTE ACCESS

11.1 If remote access is required, you must contact the Network Manager to set this up.

11.2 You are responsible for all activity via your remote access facility.

11.3 Laptops and mobile devices must have appropriate access protection, i.e. passwords and encryption, and must not be left unattended in public places.

11.4 To prevent unauthorised access to our systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone.

11.5 Select PINs that are not easily guessed, e.g. do not use your house or telephone number, and do not choose consecutive or repeated numbers.

11.6 Avoid writing down or otherwise recording any network access information where possible. Any information that is written down must be kept in a secure place and disguised so that no other person is able to identify what it is.

11.7 Protect our information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-office environment.

11.8 Users of laptops and mobile devices are advised to check their car and home insurance policies for the level of cover in the event of equipment being stolen or damaged. Appropriate precautions should be taken to minimise risk of theft or damage.

11.9 Care should be taken when working on laptops in public places (e.g. trains) that any employee or client details are not visible to other people.

12. ELECTRONIC MONITORING

12.1 You may find that you have access to electronic information about the activity of colleagues. Any such information must not be used by unauthorised individuals to monitor the activity of individual employees in any way (e.g. to monitor their working activity, working time, files accessed, internet sites accessed, reading of their email or private files, etc.) without their prior knowledge. Exceptions are:

12.1.1 In the case of a specific allegation of misconduct, the Executive Principal can authorise accessing of such information when investigating the allegation;

12.1.2 When the IT Team cannot avoid accessing such information while fixing a problem, but this will only be carried out with the consent of the individual concerned.

13. ONLINE PURCHASING

13.1 Any users who place and pay for orders online using personal details do so at their own risk and we accept no liability if details are fraudulently obtained whilst the user is using our equipment.

14. CARE OF EQUIPMENT

14.1 Do not rearrange the way in which equipment is plugged in (computers, power supplies, phones, network cabling, modems etc.) without first contacting the Network Manager.

15. AGREEMENT

15.1 All employees, contractors or temporary employees who have been granted the right to use our ICT systems are required to read and follow this policy.