D&S IFCA Technology Policy

Revised for the introduction of GDPR regulations

April 2019

Contents

Edition	Date	Comments
NJT 01	May 2018	Revised for the introduction of GDPR
NJT 02	14th December 2018	Reviewed and refined
NJT 03	3rd April 2019	Reviewed, minor amendment

D&S IFCA Policy Documentation

1. Introduction

This Policy is interlinked with the D&S IFCA Data Protection Policy. This policy applies to all employees and other ICT users, including volunteers, agency staff, visitors and members, of Devon and Severn Inshore Fisheries and Conservation Authority (D&S IFCA). It sets out the expectations of D&SIFCA in relation to the use of technology in the organisation, including email, internet and mobile devices.

2. Policy Overview

a) D&S IFCA encourages the use of ICT (Information and Communications Technology) at work. However, there are risks associated with ICT use, such as the risk of computer viruses, security breaches, the dissemination of libellous information and inappropriate personal use. This policy is designed to limit the potential impact of these risks to the organisation.

b) A breach of this policy could lead to one or more of the following actions:

- For employees, any alleged breach would be dealt with through the Disciplinary Policy and Procedure, which ultimately could lead to dismissal
- For non-employees a breach could lead to termination of the working arrangement
- D&S IFCA could remove or deny access to ICT systems, the internet or email at work or through D&SIFCA equipment.

c) Inappropriate use of ICT may also leave individuals personally at risk of prosecution

3. Principles

The following principles will apply to the operation of this policy:

a) All employees and managers will be committed to this policy and are responsible for ensuring that it is effective and complied with
b) All employees of D&S IFCA are also responsible for ensuring that other users of ICT, such as guests of D&S IFCA, comply with this policy
c) Any ICT user who is unsure about whether something he/she proposes to do might breach this policy should seek advice from his/her manager.
d) All employees will adhere to the information management systems developed and introduced by D&S IFCA (Staff catalogue, use of shared server and secure files)
e) Support and training will be available where necessary.

4. Access and Security

a) It is a criminal offence under the Computer Misuse Act (1990) to try to get unauthorised access to information or systems. ICT users must not attempt to hack into a computer or system or use these skills to commit other crimes. Also, ICT users must not delete or change data or software without authority or permission, with malicious intent, including writing or introducing any viruses or malicious programs.
b) All users of D&S IFCA's ICT systems will be given a password to enable access. ICT users are responsible for their passwords and must keep them confidential and not write them down in any identifiable way.
c) Individual passwords for personal computers must be amended each month with amended password details collated by the Intelligence Officer and Chief Officer
d) All ICT users must take reasonable precautions to ensure that their computer is not used by any unauthorised person.
e) The ICT user must be 'logged off' or the computer should be 'locked' if the ICT user is away from their desk for any sustained period of time.
f) All shared, sensitive, confidential information and personal data should be stored on the network drive (shared sever) rather than on the hard drive of an individual computer.
g) All shared, sensitive, confidential information and personal data should be stored and processed to conform with the D&S IFCA Information Management System (Policy).
h) Any laptops must be securely stored when not in use.
i) All USB data sticks should be secure when not in use

5. Hardware and Software

a) All D&S IFCA computers have software installed on them that has been correctly installed and properly licensed. Authorisation must be obtained before any programs or software are downloaded onto D&S IFCA equipment
b) ICT users must take precautions to prevent and detect malicious software, by not disabling the anti-virus software installed on D&S IFCA computers and ensuring that any potential viruses or malicious programmes are reported immediately.
c) Employees should ensure that their computer is shut down and switched off when work for the day is completed. This ensures that updates and security patches are activated when the computer starts up again and avoids wasting energy. Password-protected screen savers must be activated when computers are left switched on and unattended.

6. Email Use

Please also refer to section 7 (circulation of sensitive and/or confidential information)

a) Emails should be treated like any other form of written communication and should therefore be appropriate, professional and meet the same standards as other published documents. ICT users should check content carefully before sending and ensure that emails are only sent to those people who really need to see them.
b) The D&S IFCA master contact data base should be referred to/used to correctly identify contact addresses rather than reliance on any personal email contacts lists that may not have been updated.
c) When you intend to send email to a group, use the BCC function when appropriate
d) ICT Users must not:

- send or forward e-mails containing libellous, defamatory, offensive, discriminatory or obscene remarks. If ICT users receive an e-mail of this nature, they must promptly notify their line manager
- knowingly instigate or perpetuate chain letters or hoax virus warnings
- import or open e-mail attachments if virus protection software loaded is not up to date
- forge or attempt to forge e-mail messages; e.g. change content of a mail message received, without making it clear that the ICT user has done so
- disguise or attempt to disguise the ICT user's identity when sending mail
- include slogans, personal views not related to work or graphics as part of the ICT user's signature.

e) In all emails sent, the ICT user should ensure that they include the corporate standard information.
f) When ICT users are absent from work for more than one working day they must make every attempt to ensure that they set up 'Out of Office' arrangements, including an alternative contact for any urgent enquiries.
g) Conduct must be professional and must not bring the name of D&S IFCA into disrepute or adversely affect its reputation, customer relations or public image.
h) ICT users are not permitted to enter into any form of contract formed through electronic offer and acceptance messages without appropriate authorisation from the Senior Management Team.

7. Circulation of Sensitive and/or Confidential Information

The D&S IFCA Information Management System (Policy) and Publication Scheme (Policy) helps Staff evaluate what is and what is not sensitive and/or confidential information.

Staff should:

- Make arrangements to use the D&S IFCA CJSM secure email account
- Use a business e-mail address rather than one which appears to be a personal and/or private one.
- Consider checking out e-mail addresses when using them for the first time by asking for an acknowledgement of a test e-mail.
- Use the word 'Confidential' at the start of the subject wording.
- Use individual e-mail addresses rather than group mail boxes. (The master D&S IFCA communication data base should be referred to as the source for the correct individual email address).
- When sending the information within an attachment, password protect the attachment if possible. Both Word and Excel have the ability to do this by using the Tools, Options, Security function. Ask the intended recipient to telephone for the password when the e-mail is received by them.

8. Internet/Website Use

a) ICT users are expected to use the Internet in such a manner to ensure that it contributes to the efficient running of D&S IFCA ICT systems.
b) Many sites that could be useful to D&S IFCA may require registration. ICT users wishing to register for work purposes are encouraged to do so but must seek permission from the Senior Management Team before doing so. Where websites require D&S IFCA to enter into licence or contract terms, express permission from the Senior Management Team must be sought before registration.
c) ICT users should only download files from the Internet when they are certain that they will not cause viruses or take an unreasonable period of time to download.
d) ICT users must ensure that they do not browse websites that contain offensive, discriminatory, obscene or indecent material.
e) Accidental discovery of offensive, discriminatory, obscene or indecent material should still be reported to the Chief Officer or Senior Management Team.
f) ICT users must only use D&S IFCA ICT equipment to participate in public forums for business purposes. Conduct must be professional and must not bring the name of D&S IFCA into disrepute or adversely affect its reputation, customer relations or public image.
g) It is illegal to download copyright articles from the internet and then send them by email without permission from the author. If a user wants to do this, they will need to ensure they have gained consent from the author and have proof of this.
h) ICT users are responsible for the accuracy and currency of any information they file on the shared server to conform with the D&S IFCA Information Management System (Policy) and should make all staff aware of any errors discovered at a later date so it can be rectified (This can affect publications).
i) (ICT users are responsible for the accuracy and currency of any information they highlight for publication on D&S IFCA's Internet site or via electronic communications.
j) All staff have a responsibility to monitor the D&S IFCA Publication Scheme and D&S IFCA Retention Policy and report issues regarding published items to the D&S IFCA website managers who will make arrangements for deleting anything which is no longer relevant or modify the display as appropriate.

9. Personal Websites, Weblogs and Social Networking Websites

a) ICT users must not write about their work on personal websites and/or 'blogs' and/or social networking websites in any way.
b) Any employees who come to the attention of the organisation for placing defamatory comments on these sites will be dealt with through the Disciplinary Policy and Procedure.

10. Telephone and Mobile Devices Use

a) D&S IFCA telephone use is monitored
b) All mobile devices must be kept secure and any PIN numbers and passwords must be changed from the default and securely retained.
c) Employees with a mobile telephone are required to keep their phone on during business hours except where driving when a hands free option can be used.

d) During meetings, employees are expected to switch off mobile telephones or place them on silent mode with the option for callers to leave a voicemail. Alternative arrangements can be discussed with the Chair of a meeting.
e) When ICT users are absent from work for more than one working day it is best practice to ensure that they set up appropriate forwarding and/or voicemail, including an alternative contact for any urgent enquiries.

11. Camera and Camera Phone Use

a) The use of visual and audio capture devices such as cameras, camera phones etc within D&S IFCA premises must not lead to any harm or embarrassment either to D&S IFCA or individuals. ICT users should also note that people have the right to privacy and confidentiality and GDPR makes it necessary to have the individual's permission to take or make use of their photograph.

b) D&S IFCA has separate standards (Policy) for the use of Body Worn Video Cameras

12. Private use of D&S IFCA ICT Equipment

a) The use of the internet, telephone and email for personal use is only permitted:

- If made outside of working hours or in lunch or extended breaks
- if it can be done at no additional cost (i.e. personal telephone calls must not be made on work telephones except in an emergency)
- if this policy is complied with when used for this purpose
- if it does not interfere with the ICT user's own work or that of colleagues
- if it does not put an extra burden on the network and affect its performance.

b) The playing of games on D&SIFCA's computers is not permitted.
c) The use of the D&S IFCA ICT equipment is not permitted in connection with any non-D&S IFCA work related commercial enterprise.
d) The storage of personal photos or other images, MP3 or video files on D&S IFCA ICT equipment is not permitted.
e) D&S IFCA will not accept any liability for any personal loss of information as a result of private ICT use.
f) D&S IFCA may seek compensation for any loss or damage to its software or hardware as a result of private ICT use.
g) Personal e-mail messages must include this disclaimer - " Devon and Severn Inshore Fisheries and Conservation Authority accepts no legal responsibility for the contents of this message. The views expressed do not reflect those of Devon and Severn Inshore Fisheries and Conservation Authority ".

13. Working Away from the Office

a) The ICT user must take care to protect the equipment and its content from damage or loss by doing the following:

- Using password protection
- Transporting and storing the equipment (including laptops) securely
- When appropriate, ensuring equipment is out of sight during transit (e.g. not leaving it visible to others in the car)
- Making sure other people do not see any confidential information displayed on the screen
- Regularly backing up information which can be done by storing it on the network or copying information to a removable memory device (e.g. USB) (Encrypted for the carriage of personal data)
- Shredding any confidential information that is printed off.

14. System Monitoring

a) D&S IFCA reserves the right to monitor ICT users' e-mail, internet and telephone usage if it reasonably believes misuse or abuse. Examples of reasons why D&S IFCA may conduct monitoring include:

- If the ICT user is absent for any reason and communications must be checked for the smooth running of the business to continue.
- If D&S IFCA suspects that the ICT user has been viewing or sending offensive or illegal material, such as material containing discriminatory terminology or nudity (although D&S IFCA understands that it is possible for ICT users inadvertently to receive such material and they will have the opportunity to explain if this is the case).
- If D&S IFCA suspects that an ICT user has been using ICT for excessive personal use.
- If D&S IFCA suspects that the ICT user is using ICT in a way that is detrimental to the organisation.
- If D&S IFCA suspects that there has been a breach of this policy.

b) D&S IFCA reserves the right to retain information that it has gathered on ICT users' use of e-mail, internet and telephone for a period of up to one year.

15. End of Employment/Work Placement

a) At the end of the employment/work placement the employee must ensure that all ICT equipment owned by D&SIFCA is returned.
b) If equipment is damaged, lost or stolen through negligence or misuse and therefore is unable to be returned fully operational then D&SIFCA retains the right to recuperate the cost of replacing the equipment from the employee's salary.

D&S IFCA Policy Documentation

Complete Policy History:	• Final draft completed by Samantha Perry, DCC HR Solutions Devon on 7 April 2011 • Reviewed on 28 November 2013 by Richard Vain • Reviewed in January 2014 by Richard Vain • Reviewed in January 2016 by Emma Gill, HR Adviser, HR ONE • Reviewed in January 2018 by Karen Stagg, HR Adviser, HR ONE • Reviewed 02/05/18 by Neil Townsend, D&S IFCA • Reviewed 14/12/18 by Neil Townsend, D&S IFCA • Reviewed 03/04/19 by Neil Townsend, D&S IFCA