Report No. 16/24
National Park Authority

Report of Head of Decarbonisation

Subject: Information & Data Security Policy and ICT User Policy

Purpose of Report

The purpose of this report is to seek formal approval from the National Park Authority of the Authority's Information and Data Security Policy.
AND the ICT User Policy

Introduction/Background

An updated Information and Data Security Policy and ICT User Policy has been approved by Management Team, has undergone a consultation process with National Park Members and staff consultation.

The policy's has been reviewed with key staff members including the Performance and Compliance Officer, IT team and Data Protection Officer.

Key changes to the policies include:

- Updated onto new format and changes.
- Changes reflect use of Microsoft 365 across the Authority and clarity on data legislation.
- Updated information about when to contact the DPO, Information Commissioners Office or IT team.
- Updated information about cyber security, use of AI, use of Authority devises and personal devices.

Financial considerations
Financial considerations related to:

- risk to IT systems of misappropriated use of ICT
- data breaches and cyber security incidents.
- ensuring that Authority's ICT infrastructure and support delivers sufficient information and data security.

Risk considerations
Currently an internal audit of information, cyber security and data protection is in process.
ICT user policy and information and data security policy are crucial to reman updated and relevant to ensure compliance and to mitigate risk such as cyber-attacks and data breaches.

The policies will be reviewed by Members every 3 years, unless significant changes occur before.

Compliance

These two policies will support the Authority to comply with following legislation:

- Data Protection Act 2018/UK GDPR
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Network and Systems Regulations 2018
- Digital Economy Act 2017
- PCI DSS Requirements

Measures within the ICT User Policy will also help with Health and Safety Compliance including reference to Display Screen Equipment.

Human Rights/Equality issues

Harassment and Discriminatory behaviour relating to use of ICT is identified within prohibited activities of ICT User Policy. Use of the internet by users that can be deemed to be of an illegal, offensive or unethical nature is unacceptable and will result in disciplinary action.

Policy notes following under Privacy Rights: “The Authority recognises users’ rights to privacy, as enshrined in the Human Rights Act and Data Protection Act 2018/ UK GDPR in routine communications in respect of personal use of IT resources, in accordance with this policy.”.

Biodiversity and Sustainability implications
Decarbonisation impact added in ICT user policy.

Welsh Language statement
Once the ICT User policy is approved the following statement will be added to the front of the policy: “This policy is available in Welsh.” and a Welsh Language version of the policy will be published alongside the English version.
The ICT User policy seeks to improve and enable staff to work through the medium of Welsh.

Recommendation
Members are asked to approve this policy.
National Park Authority of the Authority’s Information and Data Security Policy.
AND the ICT User Policy

Author: Jessica Morgan
Consultees: All Staff, All members, Managment Team, IT team and DPO.

Polisi Corfforaethol
Corporate Policy

Pembrokeshire Coast National Park Authority

POL_IG2 Information and Data Security Policy

Version	Active Date	Document Owner	Internal/ External
3		Head of Decarbonisation	Internal

Please note: Policy Control Sheet is at the end of the document. Policy document is uncontrolled once printed. Please refer to the Authority's Intranet site for up-to-date policy.

Does this Policy relate to me:

- All staff, Members, contractors, consultants, temporary workers, volunteers and any other person or entities that use the Authority's IT resources.
- Technical aspects of this policy should inform the work of the IT Team.

Quick Reference - Key Policy Messages:

- This policy sets out the Authority's mechanisms for Information Security that ensure business continuity and minimise damage by preventing and minimising the impact of security incidents.

Contents

1. Policy Statement

1.1 This policy sets out the Authority's mechanisms for Information Security that ensure business continuity and minimise damage by preventing and minimising the impact of security incidents.

To carry out its various functions and services the Authority holds:

- Personal data about individuals;
- Special category data about individuals;
- Confidential Data;
- Commercially Sensitive Data.

The Authority is also required to respond to:

- Freedom of Information Requests;
- Subject Access Requests.

The data stored in electronic systems used by the Authority represent a valuable asset. The need to transmit information across networks, move data on various media and the use of portable devices increases the risk of data being vulnerable to accidental or deliberate unauthorised modification or disclosure.

In the first instance users should address questions concerning what is acceptable to their line manager or the IT Team or if it relates to personal data, the Authority's Data Protection Officer.

This policy applies to all information held in both manual and electronic form.

These three principles underpin the policy:

a) Both the public and employees have the right to respect for their privacy and hence an expectation that information about them will be treated as confidential.
b) All system assets should operate correctly, according to specification and in the way the current user believes them to be operating.
c) Information should be delivered to the right person at the right time in a secure manner where appropriate.

2. Aim of Policy

2.1 The aim of this policy is:

a) To ensure every Authority IT resources user has a proper awareness and concern for the security of IT resources and an adequate appreciation of their responsibility for information security.
b) To ensure all contractors and their employees have a proper awareness and concern for security of Authority information.

c) To provide a framework giving guidance for the establishment of standards, procedures and computer facilities for implementing security of IT resources.

d) To meet the general objectives of ISO/IEC 27002 Code of Practice for Information Systems Security.

e) To specify Authority responsibilities.

f) To ensure Authority IT resources users have an awareness of the Data Protection Act (2018) and its implications.

g) To ensure that Authority IT resources users have an awareness of the Computer Misuse Act 1990 and Digital Economy Act 2017.

h) To ensure that all Authority IT users are aware of their accountability and are aware that failure to comply with this Policy is a disciplinary offence, which may include action up to and including summary dismissal. Any action taken will conform to the appropriate Authority Human Resource policies.

i) To ensure compliance with PCI DSS Requirements

3. Scope of Policy

3.1 The Policy applies to all employees and Members of the Authority. It also applies to volunteers, contractors and visitors, not employed by the Authority but engaged to work with, or who have access to, Authority information, e.g. third party support.

3.2 Responsibility for communicating the policy lies with the induction process for staff and Members, and the relevant service manager for contractors, volunteers and visitors. Periodic reminders will be issued to raise awareness of the policy.

3.3 The Policy applies to all locations from which Authority systems are accessed (including home use) and to all devices.

3.4 Where there are links to enable non-Authority organisations to have access to Authority information, the Authority must confirm the security policies they operate under meet our security requirements or the risk is understood and mitigated.

3.5 The Policy applies to all systems and all information.

3.6 The Authority reserves the right to monitor, log, collect and analyse the content of all transmissions on networks maintained by both IT and individual departments and organisations at any time deemed necessary for performance, security measures, fault diagnostic and IT acceptable use compliance purposes.

4. Definitions

4.1 Definitions of the terms used in this policy:

4.2 “IT Resources”: All the Authority’s computing and communications systems. Specifically, IT includes, but is not limited to:

a) Physical, virtual, or hosted servers;
b) Workstations, standalone computers, laptops, printers, mobile phones, tablets and other portable computer devices;
c) Remote (“cloud”) storage and systems, peripherals, software, and data files;
d) All internal and external computing and communications networks; including telephone systems, the internet, online services, email systems, local and wide area networks, that may be accessed directly or indirectly from the Authority’s IT resources.

4.3 “Users” refers to all staff, Members, contractors, consultants, temporary workers, volunteers and any other person or entities that use the Authority’s IT resources.

4.3 Confidential data in this policy is defined as information relating to living individuals or commercially sensitive information, which, if compromised, may:

a) Result in physical, material or non-material damage to individuals such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymization, damage to reputation, loss of confidentiality (GDPR/ Data Protection Act 2018);
b) Damage the reputation of the Authority, in the locality or in the wider national press;
c) Cause the Authority to not meet its legal obligations; or compromise network security.

4.4 LAN is defined as the Authorities internal network at all locations.

5. Legislation

5.1 Some aspects of information security are governed by legislation, including:

a) The Data Protection Act (2018) and UK GDPR;
b) Copyright, Designs and Patents Act (1988);
c) Computer Misuse Act (1990);
d) Regulation of Investigatory Powers Act (2000);
e) Freedom of Information Act (2000);
f) Human Rights Act (2000);
g) BS7799 (or ISO 27002) Code of Practice for IS security;
h) Digital Economy Act (2017);
i) Privacy and Electronic Communications Regulations 2003;
j) Common law duty of confidentiality: Employer’s common law duty to employees to maintain a relationship of mutual trust and confidence.

6. Authority’s Information Security Principles

6.1 The Authority’s information Security Principles are that:

a) Information will be protected against unauthorised access;
b) Confidentiality of information will be assured;
c) Integrity of information will be maintained;
d) Regulatory and legislative requirements will be met;
e) Information Security Training will be provided;
f) All breaches of Information Security will be reported to and initially investigated by the IT Team;
g) Standards will be produced to support the policy. These include virus controls and passwords;
h) Business requirements for the availability of information and information systems will be met;
i) The Head of Decarbonisation has direct responsibility for maintaining the policy and providing advice and guidance on its implementation;
j) All Managers are directly responsible for implementing the policy within their business areas, and for adherence by their staff;
k) It is the responsibility of each user to adhere to the Information and Data Security Policy and promptly report any incidents which may have an IT security or data protection implication for the Authority.

7. Security Measures

7.1 Virus Control

a) Introducing malicious software to an individual computer or network is a criminal offence under the Computer Misuse Act 1990.
b) All PCs, laptops and servers have anti-virus software installed.
c) Where a virus is detected, this will be reported immediately to IT. If the anti-virus software cannot remove it the IT Team will manually clean the affected unit.
d) All external devices are automatically scanned upon insertion into any device that has the corporate anti-virus software installed.
e) Any removable media sent to anyone or any organisation outside the Authority must be virus scanned first.

7.2 Protection of Hardware from Theft

a) The server room is always locked and only accessible by appropriate personnel.
b) An asset register of IT Resources is maintained by the IT Team under whose responsibility the equipment is placed.
c) IT equipment should never be removed from any Authority sites without the approval of the IT Team – except for laptops and mobile devices such

as smart phones and tablets which are the responsibility of each named individual user.

d) Hardware placed in vulnerable areas or containing sensitive data should make use of physical security measures such as locked doors or physically fixing the asset to desks.

e) Redundant hardware containing data storage capability will be disposed of with a licenced waste disposal company who will provide a certificate of data destruction.

7.3 Protection of Data from Hardware Loss

a) Backups of data will be taken on a regular basis; data will be replicated where appropriate to a secure offsite location.

b) All Authority data must be stored in the appropriate location. Finalised Authority documents should not be saved on onedrive or any local storage. If in doubt users should ask their line manager / IT team.

c) All laptops that contain personal data are taken off premises must be encrypted where encryption is supported.

d) Backup media will at regular intervals be stored offsite.

e) Backup recovery procedures will be tested on a regular basis as determined by the IT Team.

f) Magnetic backup media should be stored in locked fireproof safes.

7.4 Protection of Data from Unauthorised Access

a) Passwords prevent unauthorised access. All users must adhere to guidance on password protection contained in the ICT User Policy.

b) Authority’s IT administration passwords are always kept separate and secure with restricted access. Measures are in place to address the need for password changes, or any risks associated with IT staff leaving.

c) Any printed reports deemed to contain sensitive information must be disposed of through the secure disposal service. Electronic reports which contain sensitive information must be stored in the appropriate file storage location.

d) Sensitive data must never be saved onto an unencrypted laptop or any other portable storage device.

e) When transferring data outside the organisation any data deemed to be sensitive must be encrypted.

f) Unauthorised access to backup media should be prevented by using physical controls where data is stored.

8. Protection of Personal Data

8.1 Data Protection Principles

8.2 The Public have a right to respect for their privacy and hence an expectation that information about them will be treated as confidential.

8.3 The Data Protection principles require that personal data shall be:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals;
b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

8.3 The Authority as a data controller is also responsible for, and must be able to demonstrate, compliance with the above principles.

8.4 In order to meet the requirements of the principles, the Authority will:

a) Observe fully the conditions regarding the fair collection and use of personal data;
b) Meet its obligations to specify the purposes for which personal data is used, listing them in the Authority’s data register (records of processing);
c) Collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements;
d) Ensure the quality of personal data used;
e) Apply strict checks to determine the length of time personal data is held;
f) Ensure that the rights of individuals about whom the personal data is held, can be fully exercised under relevant laws;
g) Take the appropriate technical and organisational security measures to safeguard personal data;
h) Ensure that personal data is not transferred abroad without suitable safeguards;

i) Have appropriate accountability mechanisms in place including appointing a data protection officer, carrying out data protection impact assessments and use of relevant clauses in contracts with data processors.

8.5 **Privacy Notices**

8.6 The Authority will, as far as is practicable, ensure that all individuals whose details are processed are aware of the way in which that information will be held, used (purpose of processing), retention period for that data and who it will be shared with. This information will be provided when personal data is first collected, whether written or verbal.

8.7 The Authority's overarching privacy notice will be made available on the Authority's website. Additional privacy notices and information will be provided where required.

8.9 **Confidentiality**

8.10 Arrangements (both manual and technology based) for the storage, disposal and handling of information must protect confidentiality. Care should be taken to ensure that unintentional breaches of confidence do not occur.

8.11 Breach of confidentiality is a serious matter that may result in disciplinary action by the Authority, legal action by a citizen or supplier and fines dispensed by the Information Commissioner's Office (ICO).

9. Reporting of IT Security Breaches

9.1 Any user can report a violation (or a suspected violation) of the above practices to the IT Team leader and the Authority's Data Protection Officer. The IT Team leader will then assess the level of risk associated with the violation and take appropriate action, possibly while liaising with the Authority's Data Protection Officer and ICO to minimise the risk and prevent re-occurrence of the violation.

9.2 Violations (suspected or actual) that may have a bearing on other Local Authorities will be reported to the IT Security Officers though Wales's Warning Advice and Reporting Point (WARP).

10. Firewalls and LAN Security

10.1 Access to the LAN from the internet is secured by use of firewalls.

10.2 The vulnerabilities of dedicated appliances deployed at the perimeter are monitored and patches applied as needed. Access to firewalls is restricted to the IT Team only.

10.3 No computer connecting to the LAN will allow ingress from the internet into the LAN.

11. Connection to other Networks

11.1 The Authority LAN will not connect to any other network unless the Authority is able to control access from outside users into the network.

12. Remote Access

12.1 Remote access for 3rd party support is controlled through VPN accounts that are disabled when not in use or via appropriate secure remote access systems.

12.2 Users who use terminal server services must not leave their session logged in unattended.

12.3 External access to terminal server services is authorised by the IT Team.

13. Software Control

13. 1 **Purchase of Software**

13.2 All software must be purchased in consultation with the IT Team and all software (including evaluation software) can only be authorised and installed by the IT Team using the local administrator account.

13.3 A register of software will be maintained by the IT Team.

13.4 Software must not be copied, as this is an infringement of copyright and therefore illegal – unless specifically permitted by the licence agreement. All software used by the Authority must comply with the relevant licensing agreement.

13.4 Particular attention must be paid to any licensing specifications or other similar conditions. Users are not permitted to enter into any agreement on behalf of The Authority. Agreements should be referred to the IT Team for approval.

13.5 Where permission to download is not explicit, to do so could be deemed to be ‘hacking’ or in breach of copyright laws and expose the Authority to civil and criminal liabilities.

14. Cloud Services

14.1 **Sharing and Sending Information**

14.2 There is a need to be able to upload and share files with other organisations and send large documents that would otherwise be too big for email.

14.3 Decentralised cloud services bring two primary threats.

a) Point of ingress into the protected network;
b) Undocumented storage locations some of which may be publicly accessible.

14.1 To mitigate the above use your OneDrive or Teams.

14.2 If another service is requested by a user the IT Team must establish why the existing cloud service is not compatible with the user's requirements in any given instance. Adherence to the existing service should always be the objective however in some cases other services may be cleared for use for a limited time – if the requirement can be established.

15. Email Security

15.1 Unlike other forms of communication there are special security issues with email including the inadvertent introduction of computer viruses/malware, spoofed emails or login requests as well as the danger of messages being read by other than the intended recipient. This is particularly so for email that may be sent or received via less secure networks such as the internet.

15.2 All users must follow the ICT User Policy. It applies to any electronic mail whether internal or issued to or received from external sources and it applies equally to internet mail as well as normal email facilities.

16. Viruses

16.1 **Checking for Viruses**

16.2 Provided all laptops and PCs within the Authority contain anti-virus software, users can assume that any attachments to email messages originating internally are virus-free. However, there is no guarantee that attachments to mail received from outside the Authority are similarly safe. Anti-virus is always one step behind the creators and distributors of viruses, as only once the structure of the virus is known can it be contained.

16.3 Any attachments to an email message can contain a virus and users must take care when dealing with attachments.

16.4 A particularly dangerous type of virus is a Trojan horse. These can arrive as email attachments and, indeed, are often attached to email claiming to enhance security. Typical actions by this type of virus include the deletion of files on the hard disks but some can locate the user's password, and anything else, by following keystrokes – a technique known as 'sniffing'. The sniffed data is then sent back to the hacker via email. While there is defence against these Trojan horses, users can also take steps to reduce the likelihood of introducing viruses of any description by following the procedures contained in the policy.

16.5 **Reporting Viruses**

16.6 Email attachments are scanned at the periphery of the network. Attachments that are infected are stripped from the email; emails which cannot be scanned are deleted. The system will notify the IT Team of any viruses detected on the network.

16.7 One area that technology cannot help with though is social engineering; some emails will alert users to viruses that do not exist or will take the form of pleas for help from hacked internet accounts - Yahoo, Hotmail, Google etc., users must only pass on such emails to the IT Team and not to any others either within or external to the Authority.

16.8 Scam emails are increasingly harder to detect and with AI the poorly worded emails are a thing of the past. Do not trust email marked as “External”, even more so when they contain web links or attachments. Never login to such a web page, unless you’ve checked its legitimacy.

17. Social Engineering

17.1 Social Engineering in the context of IT security is understood to mean the art of manipulating people into performing actions or divulging confidential information. This largely occurs through the means of email. Some techniques used:

a) **Phishing:** This is the most common form of attack. Typically, the acting agent sends an email that appears to come from a legitimate business—a bank, or credit card company—requesting "verification" of information and warning of some dire consequence if it is not provided. The email may also appear to come from someone you know.

b) **Baiting:** This is a technique used to install malicious software on a system and relies on an individual’s greed or curiosity. A disc, memory stick or other is left by the attacker and is picked up and placed in a machine which then becomes infected.

c) **Pretexting:** An invented scenario often communicated to the target by email. A common story being that of a person stuck abroad asking for monetary assistance.

17.2 Additionally users should beware of any website that advises them that their computer is infected with a virus.

17.3 As part of the IT induction new users will be trained to look out of specific types of attacks.

18. USB and Removable Media

18.1 Any media that contains information deemed to be sensitive should not leave the offices unless it has been encrypted. Media in this case includes CDs, DVDs, solid state drives such as USB memory sticks, any form of memory card, laptops, hard drives, phones. Personally owned USB memory sticks should not be connected to Authority equipment unless they have been virus checked by IT.

18.2 Cameras that may have captured personal specific data should be wiped as soon as they are in HQ.

19. Laptops and Mobile Devices

19.1 All previous policy statements apply to laptops they are vulnerability to theft or loss users must adhere to security measures outlined in the ICT user policy regarding laptop security measures.

19.2 Users across the Authority use smart mobile phone and tablet devices. These devices are mobile in nature and will be used in a variety of locations and will link with different Wi-Fi networks.

19.3 Users of mobile phones or tablet devices must ensure that:

a) Mobile phones and tablet devices are not left unsecured;
b) Mobile phones and tablet devices are secured with a passcode;
c) Data is only carried on a device that is essential to a users' role in the Authority;
d) If unauthorised access is suspected the user must report this to the IT team;
e) No unauthorised apps are installed onto the device;
f) Where email accounts and contacts are merged, caution is exercised to ensure that emails are never sent to an incorrect contact. A user might think they are emailing a document to a colleague when they may have in fact sent it to a personal contact;
g) They use the device in a proper fashion e.g. the device should not be rooted. Rooting or jailbreaking a device is to remove limitations placed on the device by the manufacture and allows access to operating system;
h) Caution is exercised if synchronising work and personal accounts. This is particularly important in cases where personal data including images are stored on a work device;
i) Users should the minimise risk of the device being lost and inform the IT Team immediately if a device is lost;
j) Photographs and videos should be deleted from mobile phone in line with the taking Photos/ Moving images protocol and Storage and Deletion Protocol for Photos.

20. Use of non-Authority issued IT Resources (Bring Your Own Device)

20.1 As a data controller, the Authority must remain in control of the personal data for which it is responsible, regardless of the ownership of the device used to carry out the processing of information.

20.2 All devices which are not owned by the Authority are precluded from connecting to the corporate network and are restricted to connecting to the internet via the Public Wi-Fi services. Authority email may be accessed on a mobile phone via an Exchange Active Sync (EAS) compatible mail application. Authority email can be accessed from any personally owned device via Microsoft Outlook Web Access (OWA).

20.3 Accessing the Authority email system and attached documents via a personally owned device (such as a phone, tablet or personal computer) presents risks to the safety of both organisational confidential data and personal data. As such a user must:

a) Ensure that phones and tablets are protected by an access pin code. In the case of access via a mail application, a 5 figure pin code is required, multiple failed attempts to input the correct code will result in the device being locked and all information may be remotely wiped.
b) Be aware of the risks associated with storing Authority data on a personal device and take responsibility for ensuring its safekeeping.
c) Make every effort to follow best practices such as ensuring that operating systems on personal devices are kept up to date and mitigate the risk of malicious applications by utilising trusted application stores to download applications.
d) Ensure that email, whether accessed via a mail application or web, is closed down when not in use.
e) Where email accounts and contacts are merged, exercise caution to ensure that emails are never sent to an incorrect contact.
f) Be aware of the risks associated with use of public Wi-Fi hotspots. When working with company confidential or sensitive information it is strongly recommended that a public Wi-Fi service is not used.
g) Report any device loss/theft or unauthorised disclosure of Authority data to the IT Team.

21. Meeting PCI DSS Requirements

21.1 The National Park recognise the critical importance of maintaining secure payment card transactions and we are committed to adhering to the Payment Card Industry Data Security Standards (PCI DSS). By complying with these standards, we ensure the protection of cardholder data and maintain the trust of our customers.

21.2 Ongoing Compliance: We are dedicated to continuous compliance with PCI DSS requirements. Our processes, systems, and practices align with the industry standards to safeguard sensitive payment information.

21.3 Card Payment Acceptance: Our ability to accept card payments is essential for our business operations. We commit to maintaining compliance to support our services.

21.4 We strive to meet compliance requirements while ensuring operational efficiency.

By adhering to these requirements, we contribute to a secure payment environment and protect both our customers and our business. More information about PCI DSS can be found here PCI_DSS-QRG-v4_0.pdf (pcisecuritystandards.org)

22. Physical Access

22.1 The National Park Authority offices are protected by physical restrictions to access. To ensure measures are effective:

a) Staff should not allow people they don’t know and who are not displaying visitor cards to follow them into the offices through the security doors;
b) When encountering people who are not staff and who are not displaying a visitor card, staff should politely challenge by asking if they need any assistance, then escort them to the Reception Foyer;
c) All staff should always display their security passes. Visitor passes are on red lanyards;
d) The server room is always locked and only accessible via credit card style key pass (security pass) held by the IT Team and the Caretaker.
e) A security pass card is also required to open the IT room office door to protect media, licence keys, equipment and maintenance machines logged in as domain administrator.

22. Roles and Responsibilities

22.1 All staff, Members, contractors, consultants, temporary workers, volunteers and any other person or entities that use the Authority’s IT resources must comply with this policy and notify IT Team of any IT security concerns.

22.2 Head of Decarbonisation will monitor implementation of this policy and ensure that the Authority’s risk register is updated to take account of any changes in risk.

22.3 The Authority’s Data Protection Officer will support the Authority to comply with best practice on keeping personal data safe and liaise with ICO if any data breaches occur.

23. Monitoring and Assurance

23.1 The Authority will periodically review and update this policy to ensure its effectiveness and relevance.

23.2 All users will be offered training on this policy upon joining the Authority and all staff will be periodically reminded of their responsibilities.

23.3 Users should report any concerns or questions related to IT security to the IT team.

23.4 Management and Members will be made aware of changes in risk through updates provided via the Authority’s risk register.

24. Related Policies and Operational Procedures

24.1 ICT User Policy

24.2 Data Protection Policy

Policy Control Sheet

Change Level

Change Level	Tick
Minor editorial/ accuracy changes	
Change requires Management Team Approval Only	
New Policy or Change requires NPA Approval / HR Committee Approval	✓

Consultation

Group	Date
Staff and Members consultation (end of consultation)	29 March 2024
Data Protection Officer	4 January 2024
Management Team	1St March 2024 & 15 March 2024

Assessments

Assessment – If Applicable	Date
Integrated Assessment – Full	
Integrated Assessment – Policy/ Procedure Review	
Data Protection Impact Assessment	

Approval

Approved by	Name	Date	Signature
[NPA/ HR Committee/ Management Team]			

Version History

Version	Active Date	Summary of Changes
2	04 September 2019	Every 3 years. Legislative/ organisational changes. Security risk changes.
3		

Review

Version	Active Date	Document Owner	Review Date Trigger
3		Head of Decarbonisation	

Publication

Policies must be co-ordinated through the Performance and Compliance Team, for compliance, auditing, and control purposes. Please send all new or reviewed policies once approved to mairt@pembrokeshirecoast.org.uk for formal publication of policy to staff, Members, volunteers and where required on the Authority's website.

Publication	Date
Published on Sharepoint Corporate Policy Hub	
External Policy – Published on Website: HTML	N/A

DRAFT VERSION

Polisi Corfforaethol
Corporate Policy

Pembrokeshire Coast National Park Authority

POL_IG1 ICT User Policy

Version	Active Date	Document Owner	Internal/ External
3		Head of Decarbonisation	Internal

Please note: Policy Control Sheet is at the end of the document. Policy document is uncontrolled once printed. Please refer to the Authority's Intranet site for up-to-date policy.

Does this Policy relate to me:

- All Authority's Members, staff, volunteers, independent contractors, agents, and any other users of the Authority's IT resources.
- The policy applies to all locations from which Authority systems are accessed (including home use) and to all devices including phones.

Quick Reference - Key Policy Messages:

- Sets out expectations for Users in terms of
  - Permitted use of IT resources and what activities are prohibited
  - Security, including passwords and risks linked to e-mails
  - Protecting equipment
  - Procurement of hardware and software, including installation
  - Legislative framework we operate in, including Data Protection and Freedom of Information
  - Use of AI
  - Supporting decarbonisation when using IT resources

Contents

1. Policy Statement

1.1 Pembrokeshire Coast National Park Authority (The Authority) relies on its Information and Communication Technology (ICT) to fulfil its remit. The Authority requires that this policy be followed to ensure that its Members, staff, volunteers, independent contractors, agents, and any other users of the Authority's systems use its IT resources legally and appropriately.

1.2 The rules and obligations described in this policy apply to all users of Authority IT, wherever they may be located and in whatever capacity they might be engaged. All Authority users will be made aware of, and asked to accept the terms of, this policy upon commencement of their employment or adoption of the policy by Authority Members as appropriate and when revisions are made.

1.3 All contractors, agents, and any other users of the Authority's systems will be made aware of this policy and asked to accept its terms prior to such third party having any access to the Authority's IT systems or data. Any violations of this policy by any member of staff or third party will be taken seriously and may result in disciplinary action, including possible employment termination, and civil and criminal liability.

1.4 It is every user's duty to use Authority IT resources responsibly, ethically, and lawfully. Correct and efficient use of IT is a requirement, not an option, consequently the Authority recognises its responsibility to train and support the users of its IT resources as appropriate to their role and capabilities. IT training need requirements will be included as part of the annual performance review.

1.5 In using or accessing IT resources, users must comply with the provisions set out in the policy.

2. Aim of Policy

2.1 The aim of this policy is to ensure that the Authority's Members, staff, volunteers, independent contractors, agents, and any other users of the Authority's systems use its IT resources legally and appropriately.

3. Scope of Policy

3.1 The policy applies to all locations from which Authority systems are accessed (including home use) and to all devices including phones.

4. Definitions

4.1 Definitions of terms used in this policy.

4.2 "IT resources": All the Authority's computing and communications systems. Specifically, IT includes, but is not limited to:

a) Physical, virtual, or hosted servers;
b) Workstations, standalone computers, laptops, printers, mobile phones and tablets and other portable computer devices;

c) Remote (“cloud”) storage and systems, peripherals, software, and data files;
d) All internal and external computing and communications networks including telephone systems, the internet, online services, email systems, local and wide area networks that may be accessed directly or indirectly from the Authority’s IT resources.

4.3 “Users” refers to all staff, Members, contractors, consultants, temporary workers, volunteers and any other person or entities that use the Authority’s IT resources.

4.4 The IT resources and information held within them are the property of the Authority and may only be used for legitimate and lawful purposes. Users are permitted access to Authority IT resources to assist them in the performance of their duties.

5. Legislation

5.1 Health and Safety – Display Screen Equipment

In accordance with the Health and Safety (Display Screen Equipment) Regulations, the Authority has a duty of care to ensure that users are protected from the health risks of working with display screen equipment (DSE), such as PCs, laptops, tablets and smartphones.

The regulations apply to users who use DSE daily, for an hour or more at a time. The regulations don’t apply to users who use DSE infrequently or only use it for a short time.

A Display Screen Self-Assessment is available on the Authority’s internal intranet– a user must discuss any concerns with their line manager who will consult with IT and People Services to find the best solution.

DSE Users should have regular eye checks, the cost of which will be paid for by the Authority.

5.2 Users must comply with the following legislation.

a) Data Protection Act 2018 / UK GDPR which sets out rules for processing of personal data and places significant obligations on organisations regarding data protection including the rights of data subjects.
b) Computer Misue Act 1990 which makes it illegal to gain unauthorised access to computer systems and networks, as well as to create or distribute malicious software or carry out cyberattacks.
c) Freedom of Information Act 2000 providing the public with information held by public authorities, including government agencies and public sector organisations. This is important in how information is handled and disclosed.
d) NIS Regulations (Network and Information Systems Regulations 2018) These regulations require organisations providing essential services to take measurements to protect their IT systems and report certain

cybersecurity incidents.

6. Permitted use of IT Resources

6.1 IT resources are the property of the Authority and may only be used for approved purposes.

6.2 Users are permitted access to IT resources to assist them in the performance of their duties.

6.3 Occasional limited and appropriate personal use of IT resources is permitted when such use does not:

a) Interfere with the user's work performance;
b) Interfere with any other user's work performance;
c) Unduly impact the operation of IT resources; or
d) Violate any other provision of this policy or any other policy, guideline, or standard of Pembrokeshire Coast National Park Authority.

6.4 Examples of appropriate personal use out of normal working hours (i.e. "clocked off" at lunch or before or after work):

a) Conducting educational or research projects
b) Performing a not-for-profit or community service
c) Participating in non-work related professional, civic or union associations
d) Retrieving news stories and information
e) Pursuing reasonable recreational interests

7. Prohibited Activities

7.1 At all times, users have the responsibility to use IT resources in a professional, ethical, and lawful manner. Users must ensure that personal use of IT resources does not have a detrimental impact on the Authority's ability to conduct its business. Personal use of IT resources is a privilege that may be monitored at the request of the manager and revoked at any time.

7.2 Material that is fraudulent, harassing, sexually explicit, profane, obscene, intimidating, defamatory, discriminatory, or otherwise unlawful or inappropriate may not be displayed, stored or transmitted using an Authority device, this includes but is not limited to: email or other form of electronic communication (e.g., messaging systems, online collaborative systems, internet searches, bulletin boards, newsgroups and chat groups). Users encountering or receiving this kind of material should immediately report the incident to their line Manager and the IT Team.

7.3 Use of the internet by users that can be deemed to be of an illegal, offensive or unethical nature is unacceptable and will result in disciplinary action e.g.,

a) Violation of copyright, license agreements or other contracts for example copying and using software for business purposes from a site where there is a clear limitation for personal use only;

b) Downloading or viewing any information which could be considered illegal or offensive e.g. pornographic or racist material;
c) Attempts made, whether successful or not, to gain unauthorised access to information resources – commonly known as 'hacking';
d) Using or knowingly allowing someone else to use any computer, mobile device, computer network, computer system, program or software to devise or execute any artifice or scheme to defraud or to obtain money, property, services, or other things of value by pretences, promises or representations;
e) Destroying, altering, dismantling, disfiguring, preventing rightful access to or otherwise interfering with the availability and/or integrity of computer-based information and/or information resources without proper authorisation;
f) Without authorisation invading the privacy or entities that are creators, authors, users or subjects of the information resources; for example reading the email of another without permission;
g) Using the internet for political lobbying;
h) Transmitting or causing to be transmitted communications that may be construed as harassment or disparagement of others;
i) Violating any UK laws pertaining to the unauthorised use of computer resources or networks.

7.4 Some degree of filtering on internet access, i.e. restriction on what sites and services are accessible, exists and may be modified or updated without notification.

7.5 Users should not at any time store personal files on Authority IT resources. It is acknowledged that such files may be temporarily present, for example when being transferred from one personal source to another, but they should not be stored for any significant period and may be permanently erased by the IT Team, or automated systems, without notice.

7.6 When using IT resources such as phones and tablets, caution must be exercised if synchronising personal accounts on these devices. Synchronisation could for example result in work photos being uploaded to personal cloud storage systems. This applies to both work issued devices and if staff are using their personal devices for Authority work.

7.7 With the exception of laptops and mobile devices such as smart phones and tablets (which are the responsibility of each named individual user), users may not remove any IT resources from Authority premises or elsewhere without the specific permission of a member of the IT Team.

7.8 When wishing to access personal email and webmail accounts, users should use their own mobile phone, tablet or other device in order access their e-mail through the public Wi-Fi.

8. Use of non-Authority issued IT resources (Bring your Own Device)

8.1 As a data controller, the Authority must remain in control of the personal data for which it is responsible, regardless of the ownership of the device used to carry out the processing of information.

8.2 All devices which are not owned by the Authority are precluded from connecting to the corporate network and are restricted to connecting to the internet via the Public Wi-Fi services. Authority email may be accessed on a mobile phone via adding an Exchange account to a compatible mail application. Authority email can be accessed from any personally owned device via browsing to “Outlook on the Web” in a web browser.

8.3 Accessing the Authority email system and attached documents via a personally owned device (such as a phone, tablet or personal computer) presents risks to the safety of both organisational confidential data and personal data. As such a user must:

a) Accept that, in the event of loss; theft or unauthorised access, should email be accessed via a mail application, the Authority has the right to disable the users access to Authority systems.
b) Ensure that phones and tablets are protected by an access pin code. In the case of access via a mail application, a minimum 5 figure pin code is required.
c) Personal devices are prohibited to be used for storing and working on Authority data. Attachments downloaded from work email e.g. via a phone or web mail, should be deleted from any personal device.
d) Make every effort to follow best practices such as ensuring that operating systems on personal devices are kept up to date and mitigate the risk of malicious applications by utilising trusted application stores to download applications.
e) Ensure that email, whether accessed via a mail application or Outlook on the Web, is closed down and or signed out when not in use.
f) Where email accounts and contacts are merged, exercise caution to ensure that emails are never sent to an incorrect contact.
g) Be aware of the risks associated with use of public Wi-Fi hotspots. When working with company confidential or sensitive information it is not permitted to use a public Wi-Fi service.
h) Report any device loss/theft or unauthorised disclosure of Authority data to the IT team.
i) Access to your Authority account from outside the UK is not by default allowed, it can be requested via an IT support ticket. Work mobile phones are not to be used for data or roaming outside of the UK – phones data settings should be set to not roam.
j) Staff that leave employment are not permitted to share company material, or any material created during employment for their personal/ future use and company documents should not be deleted from personal folders/ drives.

9. Security

9.1 Passwords prevent unauthorised access. Users are responsible for safeguarding their login credentials and must not share them with others. Passwords that have been divulged to, or changed by, the IT Team should be changed again afterwards by the user.

9.2 Passwords must be changed if you suspect that it has been compromised. If you have lost control of the account, you must contact IT. Passwords can only be changed from a device connected to the corporate network at a PCNPA site.

a) Passwords should have the following characteristics:
  - ➢ At least ten characters long;
  - ➢ Must not be a previous password;
  - ➢ Must be generated by the user;

b) Users should follow this guidance when creating passwords:
  - ➢ Use a unique password for each of your important accounts;
  - ➢ Use a mix of letters, numbers, and symbols in your password – deriving these from a phrase that has meaning for you is a good way of ensuring memorability;
  - ➢ Don’t use personal information or common words as a password;
  - ➢ Make sure your backup password options are up-to-date and secure;
  - ➢ Keep your passwords secure.

9.3 Users must lock their computer screens when leaving their workstations unattended. Users who use cloud-based systems must not leave their session logged in unattended.

9.4 The use of personal USB drives or external devices on PCNPA computers is prohibited without prior authorisation. Should a device be connected, it is subject to the same antivirus scanning and potential quarantine / deletion of files, for which the Authority is not responsible.

9.5 Users must not attempt to connect any found portable storage drives or USB drives. These must be handed in to IT.

9.6 Users must report any suspected security breaches or incidents immediately to the IT department**.**

9.7 Users are responsible for ensuring their laptops are securely stored whilst away from work premises.

a) Devices must not be left unattended i.e. in a car, or unsecured when in the office or even at home or a hotel room;

b) They must only be used by users, not by family or friends;

c) Any work done offsite should be synced with work on the main file system as soon as possible;

9.8 Users must only share data externally with authorised persons. This includes email, OneDrive and Teams sharing. Staff should apply sensitivity labels to high-risk content. (inset hyperlink to guidance on what these are and how they should be used)

10. Protection of Equipment from Accidental Damage

10.1 Care must be taken when eating or drinking near IT equipment. No food or drinks should be consumed in the server room.

10.2 The location of all hardware should comply with Health and Safety standards; trailing cables should be secured, and desk surfaces must be stable. Advice on this can be obtained from the Authority's People Services team.

10.3 All user devices such as PCs and printers should be switched off when not in use for extended periods unless required to remain on. ICT infrastructure hardware, for example severs, should remain on

10.4 Magnetic media should not be placed next to laser printers, photocopiers or any other device that creates electromagnet disruption.

10.5 Air vents on computers should not be obstructed. Equipment should not be placed in an environment where dust intake could be excessive.

10.6 It is users' responsibility to ensure equipment is kept externally clean and dust free, the IT Team can provide guidance and products on request.

10.7 Any labelling attached to equipment must not be removed

10.8 Any damage to equipment should be immediately reported to the IT Team**.**

11. Decarbonisation

11.1 The IT team will promote the use of energy-efficient hardware and users are encouraged to turn off equipment when not in use. Laptops should be shut down at the end of the day and not just close the lid.

11.2 The Authority encourages remote work and video conference to reduce the need for physical office spaces and commuting.

11.3 Print only when necessary. Paperless workflows and digital documentation is encouraged. However, for each digital action there is a carbon cost, therefore staff are encouraged to limit the sending of large attachments or unnecessary "ok thanks" emails. Use a collaborative digital platform (Teams) to avoid attachments.

11.4 Virtualization and Cloud Services: Staff should only save documentation that is necessary to save and use OneDrive, teams and Sharepoint on cloud services where possible to reduce the need for physical servers and data centres.

12. Procurement of Hardware and Software

12.1 The IT Team must approve all IT related hardware purchases. This is to ensure that:

a) All purchases are registered with the Hardware Database to allow adequate tracking and management of resources;
b) All systems are of a standard that allows streamlined technical support procedures;
c) Optimal purchase prices are achieved through corporate discount schemes;
d) Data Protection considerations have been considered and risks assessed in accordance with the Information and Data Security Policy. IT may request that a Data Protection Impact Assessment is completed prior to approving a IT related hardware purchases.
e) No software should be downloaded from or via the internet unless doing so is expressly permitted by the IT Team and it is in connection with the user's job.

12.2 Users must not evaluate, tender for, order or purchase any new software or software development (e.g. web sites) without prior consultation with the IT team leader.

12.3 This is to ensure that all systems are fit for purpose, appropriate technology is used, existing IT resources are capitalised on wherever possible, information governance security considerations are considered, and appropriate support and maintenance agreements are made.

13. Installation of Software

13.1 The IT Team must approve all new software installed on any of Authority's system. Software must be installed by a member of the IT Team via a request to the IT Helpdesk. This is to ensure that:

a) The Authority is fully licensed for all software in use;
b) All software is compatible with other software running on the same system(s);
c) All equipment is protected from computer viruses, worms and unsolicited email (spam);
d) All software is registered in the Software Database to allow for organised storage and retrieval;
e) Data Protection considerations have been considered and risks assessed in accordance with the Data Protection Policy. IT may request that a Data Protection Impact Assessment is completed prior to installing software.

14. Computer Viruses / Malware / Phishing

14.1 Users must complete all IT training including cyber security, as directed by their line manager and HR.

14.2 All users must always run Authority’s approved anti-virus software. Disabling this software is considered a serious breach of this policy, as it constitutes a risk to IT resources.

14.3 Any notifications or alerts regarding new viruses must be referred only to the IT Team for them to confirm the validity of the alert and prevent the waste of time and resources caused by hoaxes.

15. Use of Artificial Intelligence (AI).

15.1 AI is becoming a bigger part of our lives, as the technology behind it becomes more and more advanced. It is important that if staff begin to use AI they understand principles and rules for safe use and if in doubt, speak to a member of the IT team.

15.2 It is important to be aware of the following,

a) Algorithmic bias: Awareness of the potential for AI systems to perpetuate biases and care should be taken when using AI to mitigate such biases during development and deployment.
b) Privacy and data protection: Knowledge of relevant privacy laws and regulations, understanding the risks associated with AI’s use of personal data, and ensuring compliance with data protection practices. When using AI software personal or sensitive business data should not be inputted into any programmes. If in any doubt, please speak to a member of the IT team.
c) Accountability and Accuracy: Understanding the need to establish clear lines of accountability for AI systems’ decisions and actions, including responsibility for errors or unintended consequences. Accuracy care should be taken to ensure AI generated work is accurate. Outputs of AI software should be considered unreliable and for indication only, and must always be verified by a human.
d) Ethical decision-making: Familiarity with ethical frameworks and principles to guide AI development and deployment, including fairness, transparency, accountability, and human well-being.
e) Social implications: Recognising the potential impact of AI on society, employment, and equity and considering measures to address these implications responsibly.

16. Privacy Rights

16.1 The Authority recognises users’ rights to privacy, as enshrined in the Human Rights Act and Data Protection Act 2018/ UK GDPR in routine communications in respect of personal use of IT resources, in accordance with this policy.

16.2 On occasion there will be issues whereby the Authority’s interests require the Authority to access users’ data or allow external agencies access to those data where they have a legal right to do so. Accordingly users should be aware that personnel of the Authority and/or legally entitled external agencies (such as the police, Wales Audit Office, Inland Revenue, HM Customs and Excise, etc.), may access and review all materials that users create, store, send, or receive on the computer or through the internet or any other computer network.

16.3 Users must never consider electronic communications to be either fully private or fully secure. Email may be stored indefinitely on any number of computers, including that of the recipient. Copies of messages may be forwarded to others either electronically or on paper. In addition, email sent to non-existent or incorrect usernames may be delivered to persons that you never intended.

16.4 Users must respect the privacy and confidentiality of all data stored on the Authority IT systems. Access to sensitive or restricted data is limited to authorised personnel only.

16.5 Many worm type virus infections misrepresent (spoof) the sender's email address, but such emails are easily identifiable by IT professionals and users will not be held accountable for the contents of any email purporting to originate from them in such cases.

16.6 The Authority reserves the right to monitor usage of its IT resources to ensure compliance with this policy and with the law. Managers and/or HR can request monitoring and logging information from IT if there is a concern about the behaviour of an individual or group of individuals.

16.7 In such cases the decision and reason(s) to implement monitoring will be recorded and the default will be to notify the affected individual(s) that monitoring is being implemented but this will not always be the case, for example if there is suspicion of gross misconduct such as a breach of the prohibited activities clause of this policy, or breach of the law.

16.8 If you have any concerns about data privacy please contact the Authority's Data Protection Officer: DPO@pembrokeshirecoast.org.uk

17. Roles and Responsibilities

17.1 Users must ensure that electronic communications are truthful and accurate to the best of their knowledge.

17.2 Users must take the same care in drafting email and other electronic documents as they would for any other written communication. The quality of your writing will reflect on our organisation. Always strive to use good grammar and correct punctuation. Further guidance is available in the Authority's Corporate Style Policy.

17.3 Users should remember that email messages can be intercepted due to the nature of the internet. It is possible to set up routines that can scan passing email for key words without being detected. Consequently, users should consider the contents of any message or attachments sent by email.

17.4 The content of email is subject to all applicable UK laws such as those relating to copyright, defamation, discrimination and harassment, data protection and public records, as well as statutes concerning the sensitive and pornographic. Nothing illegal or infringing a third party's intellectual property rights should be included in an email.

17.5 Email should not be relied upon as a method of emergency communication. Any critical communication sent via email should be confirmed by phone.

17.6 It is important to know who you are talking to. Although this may seem obvious, users should always look at the actual sender address at the top of the email before reading, and perhaps reacting to the message itself. Consider does the message fit with previous or expected communications, would this individual ask you to click a link?

17.6 Users must not click on links or download attachments unless they know the sender and are confident the email is from that sender.

17.7 Attachments and links in emails must be treated with caution, and users should not download or click on suspicious content.

17.8 Users must keep in mind that anything created or stored on IT resources may, and likely will, be reviewed by others.

18. Monitoring and Assurance

18.1 The Authority will periodically review and update this policy to ensure its effectiveness and relevance.

18.2 All users will be offered training on this policy upon joining the Authority and all staff will be periodically reminded of their responsibilities.

18.3 Users are encouraged to report any concerns or questions related to IT security to the IT team.

19. Related Policies and Operational Procedures

19.1 Display Screen Self-Assessment

19.2 Corporate Style Policy

19.3 Information and Data Security Policy

19.4 Data Protection Policy

Policy Control Sheet

Change Level

Change Level	Tick
Minor editorial/ accuracy changes	
Change requires Management Team Approval Only	
New Policy or Change requires NPA Approval / HR Committee Approval	√

Consultation

Group	Date
Staff and Members Consultation Staff Reps group	29 March 2024 14th March 2024
Data Protection Officer	4th January 2024
Management Team	1st March 2024 & 15 March 2024

Assessments

Assessment – If Applicable	Date
Integrated Assessment – Full	
Integrated Assessment – Policy/ Procedure Review	
Data Protection Impact Assessment	

Approval

Approved by	Name	Date	Signature
[NPA/ HR Committee/ Management Team]			

Version History

Version	Active Date	Summary of Changes

Review

Version	Active Date	Document Owner	Review Date Trigger

Publication

Policies must be co-ordinated through the Performance and Compliance Team, for compliance, auditing, and control purposes. Please send all new or reviewed policies once approved to mairt@pembrokeshirecoast.org.uk for formal publication of policy to staff, Members, volunteers and where required on the Authority's website.

Publication	Date
Published on Sharepoint Corporate Policy Hub	
External Policy – Published on Website: HTML	N/A