**External and Internal**

**Policy**

**Review**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Effective Date** | **Document Owner** | **Review Date Trigger** |
| 2 | 04 September 2019 | Business Improvement and IT Manager | Every 3 years.  Legislative/ organisational changes. Security risk changes. |

**Target Audience**

All users of Authority IT.

**Consultations**

|  |  |
| --- | --- |
| **Group** | **Date** |
| Staff Reps | 9 August 2019 |

**Approvals**

This document requires the following approvals.

|  |  |  |  |
| --- | --- | --- | --- |
| **Approved by** | **Name** | **Date** | **Signature** |
| Leadership Team | On File | 25 June 2019 | On File |
| National Park Authority | On File | 4 September 2019 | On File |

|  |
| --- |
| **Contents** |

[1. Policy Statement 3](#_Toc18499117)

[2. Purpose and Scope 3](#_Toc18499118)

[3. Definitions 4](#_Toc18499119)

[4. Authority’s Duty of Care 4](#_Toc18499120)

[5. Users’ Duty of Care 5](#_Toc18499121)

[6. Permitted use of IT Resources 5](#_Toc18499122)

[7. Prohibited Activities 6](#_Toc18499123)

[8. Use of non-Authority issued IT resources (Bring your Own Device) 7](#_Toc18499124)

[9. Procurement of Hardware 8](#_Toc18499125)

[10. Procurement of Software 8](#_Toc18499126)

[11. Installation of Software 8](#_Toc18499127)

[12. Computer Viruses 9](#_Toc18499128)

[13. Privacy Rights 9](#_Toc18499129)

[14. Reference 10](#_Toc18499130)

[15. Version History 10](#_Toc18499131)

|  |
| --- |
| Policy Statement |
| 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.  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.  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.  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.  **In using or accessing IT resources, users must comply with the provisions set out in the policy.** |

|  |
| --- |
| Purpose and Scope |

2.1 The purpose 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.

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

|  |
| --- |
| Definitions |

Definitions of terms used in this policy.

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

1. Physical, virtual, or hosted servers;
2. Workstations, standalone computers, laptops, printers, mobile phones and tablets and other portable computer devices;
3. Remote (“cloud”) storage and systems, peripherals, software, and data files;
4. 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.

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

3.3 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.

|  |
| --- |
| Authority’s Duty of Care |

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.

* 1. A Display Screen Self-Assessment [1] is available on the Authority’s internal website (Parcnet) – a user must discuss any concerns with their line manager who will consult with IT and Personnel to find the best solution.
  2. DSE Users should have regular eye checks, the cost of which will be paid for by the Authority.

|  |
| --- |
| Users’ Duty of Care |

**What is the User’s duty of care?**

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

5.2 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 Guide [2].

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

|  |
| --- |
| Permitted use of IT Resources |

**What is permitted with our computers?**

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:

1. a) Interfere with the user’s work performance;
2. b) Interfere with any other user’s work performance;
3. 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.

**What is appropriate personal use?**

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

1. Accessing personal webmail, e.g. Gmail, Outlook, etc.;
2. Accessing social media sites;
3. Online shopping;
4. Performing a not-for-profit or community service;
5. Participating in non-work related professional, civic or union associations;
6. Conducting educational or research projects;
7. Retrieving news stories and information of general  
   interest;
8. Pursuing reasonable recreational interests;

|  |
| --- |
| Prohibited Activities |

**Conduct**

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.

**What activities are prohibited?**

7.2 Material that is fraudulent, harassing, sexually explicit, profane, obscene, intimidating, defamatory, discriminatory, or otherwise unlawful or inappropriate may not be sent by email or other form of electronic communication (e.g., messaging systems, online collaborative systems, bulletin boards, newsgroups and chat groups) or displayed on, or stored in, the Authority’s IT systems. Users encountering or receiving this kind of material should immediately report the incident to their Supervisor/ Manager and/or the IT Team.

**Are some sites or services restricted?**

7.3 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.

**Storage of files on Authority resources**

7.4 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.

**Synchronising Personal Accounts on Devices used to carry out Authority work**

7.5 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.

**Removal of IT resources**

7.6 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.

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

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.

8.1 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).

8.2 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:

1. 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 seek to remotely wipe all information from the phone.
2. 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.
3. Be aware of the risks associated with storing Authority data on a personal device and take responsibility for ensuring its safekeeping.
4. 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.
5. Ensure that email, whether accessed via a mail application or OWA, is closed down when not in use.
6. Where email accounts and contacts are merged, exercise caution to ensure that emails are never sent to an incorrect contact.
7. 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.
8. Report any device loss/theft or unauthorised disclosure of Authority data to the IT team.

|  |
| --- |
| Procurement of Hardware |

**Who approves IT hardware purchases?**

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

1. All purchases are registered with the Hardware Database to allow adequate tracking and management of resources;
2. All systems are of a standard that allows streamlined technical support procedures;
3. Optimal purchase prices are achieved through corporate discount schemes;
4. Data Protection considerations have been taken into account and risks assessed in accordance with the Data Protection Policy [3].

|  |
| --- |
| Procurement of Software |

10.1 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 manager or relevant member of IT Team. 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 taken into account and appropriate support and maintenance agreements are made.

|  |
| --- |
| Installation of Software |

**Who must approve software installation?**

11.1 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:

1. The Authority is fully licensed for all software in use;
2. All software is compatible with other software running on the same system(s);
3. All equipment is protected from computer viruses, worms and unsolicited email (spam);
4. All software is registered in the Software Database to allow for organised storage and retrieval;
5. Data Protection considerations have been taken into account and risks assessed in accordance with the Data Protection Policy [3].

|  |
| --- |
| Computer Viruses |

**What about viruses?**

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

12.2 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.

|  |
| --- |
| Privacy Rights |

**Do I have any rights to privacy?**

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

13.2 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.

**Are my emails private and secure?**

13.3 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.

13.4 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.

**Will I be monitored?**

13.5 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.

13.6 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 in the event that there is suspicion of gross misconduct such as a breach of the prohibited activities clause of this policy, or breach of the law.

**Data Protection Officer**

13.7 If you have any concerns about data privacy please contact the Authority’s Data Protection Officer: [DPO@pembrokeshirecoast.org.uk](mailto:DPO@pembrokeshirecoast.org.uk)

|  |  |  |
| --- | --- | --- |
| Reference | | |
| 1 | Display Screen Self-Assessment | <http://parcnet/Docs/Documents/Display%20screen%20self%20assessment.doc>  (Internal Document) |
| 2 | Corporate Style Guide | [http://parcnet/Docs/Documents/Corporate Style Guide.docx](http://parcnet/Docs/Documents/Corporate%20Style%20Guide.docx) (Internal Document) |
| 3 | Data Protection Policy | [*https://www.pembrokeshirecoast.wales/Files/files/Corporate%20Docs/POL\_006%20Data%20Protection%20Policy%20V2.docx*](https://www.pembrokeshirecoast.wales/Files/files/Corporate%20Docs/POL_006%20Data%20Protection%20Policy%20V2.docx) |

|  |  |  |
| --- | --- | --- |
| Version History | | |
| Version | Effective Date | Summary of Changes |
| 2 | 04 September 2019 | * Standard Template applied. * Section 7 – Terms under which non authority issued IT resources may be used clarified. |