Peak District National Park Authority
Information Management Policies Framework

Version	Publish Date	Amendment History
4.0	18/05/2018	
4.1	16/11/2018	Updated links to survey and included changes to provision of passwords by IT re: problem resolution.
4.2	01/02/2019	Include advice about setting up auto-acknowledgement for email
4.3	30/08/2019	Inclusion of section on requesting permission to access user's mailbox in their absence
4.4	28/10/2019	Entry in section on use of email regarding use of Peak District email address for commercial gain or personal financial transactions. Re-edit to meet new accessibility guidelines.
4.5	04/09/2020	Revised for accessibility issues
5.0		Review and update to account for latest legislation and technology.

Who needs to read and adhere to this Policy?

This Policy applies to everyone with access to PDNPA hardware, systems or data (electronic data as well as data in any other format).
It sets out the appropriate use of Peak District ICT hardware, services and data.
It explains your responsibilities and provides guidance on appropriate use.

What we expect from you - Know the rules and follow them:

Equipment, data and services are used appropriately
Use information responsibly:

- If required, obtain consent to use someone's information
- Safeguard your personal data and that of other people
- Ensure personal and sensitive information is kept confidential
- Maintain the integrity, confidentiality and quality of information
- Ensure you comply with any regulatory and legislative requirements

Be yourself:

- Keep your PDNPA account details secure
- Always use your own account for access
- Keep data secure and protected against unauthorised access

Protect:

- Secure and protect ICT systems and data against unauthorised access
- Report all breaches of information security, actual or suspected
- Work in ways that meet regulatory and legislative requirements
- Follow our clear desk policy

Heads of Service and Team Managers are responsible for ensuring staff, within their business areas, are working in accordance with and have signed up to the ICT policies.

What to expect from us

ICT service level agreement (Appendix 2)
Guidelines for the use and security of our systems are in place.
All breaches of information security, actual or suspected, are investigated.
(*Breaches of ICT policies will be handled in accordance with the Authority's Disciplinary Procedures.)*

Acceptance & review

You are required to complete an **on-line form**

The framework is reviewed, amended and updated as we adopt changes in technology and to comply with revised legislation. We will make you aware of any significant or material changes. If you have any questions or would like additional information then please contact the PDNPA IT team.

Introduction

This framework brings together the policies related to managing information and the appropriate use of ICT services.

This document;

- summarises your responsibilities
- provides summary guidance for managing information
- ensures you know how to protect yourself online
- explains how to make best use of our technology and ICT systems
- links to Policy documents and Guidance Notes

This document is in four sections:

1. Security
   How we keep information and systems safe.

2. Acceptable Use and ICT monitoring
   What you agree to do when using PDNPA ICT hardware, software, data and systems. How that use is monitored, recorded and reported.

3. Data and Records Management
   How we expect you to manage information. Standards and guidance to ensure data and records meet our business needs and legal requirements.

4. Advice and Guidance
   Tips, policies and know how. Utilise ICT and Support services as effectively as possible.

Contents Page

Section 1 Security: keeping information & systems safe

Purpose – Our data is a valuable asset and all staff need to adopt measures to protect both the confidentiality and integrity of PDNPA data and the network.

Summary of your responsibilities

a. Complete data protection and security training within set deadlines
    a. Completion is a prerequisite for access to PDNPA ICT services.
    b. You are responsible for protecting the data you use.
b. Understand and identify sensitive data - if you are unsure, do not assume, ask someone
    a. You are accountable for any action taken in relation to the data you work with
c. If you observe anything unusual or suspect a breach, report it to your Line Manager or IT Support
d. Data is secured when transported or transferred
e. Lock your computer when not in use (Windows key + L = lock)
f. Protect equipment from theft and damage, including spills
g. Do not store data on your computer (Local Disks) as it is not backed up
    a. Store files and folders in the appropriate share on the server
    b. New data assets should be recorded in Informu the Information Asset Register
h. PDNPA equipment, including mobile phones, and email is for PDNPA work only
    a. Do not use Authority equipment for non-Authority work
    b. only use removable media that has a PDNPA asset sticker
i. Equipment should be used in a secure and legal manner, in a trusted environment
j. Software should be used in accordance within the terms of the license
k. Abide by the Computer Misuse Act – law governing the way in which individuals can lawfully access data on a device
l. Password Management
    a. Do not use your PDNPA password for online accounts
    b. Do not write down or share your password(s)

Password Policy

a. PDNPA IT enforces settings for access to our computer network, including the maximum age of the password.
    a. These settings must also be used for 3rd party applications and services.
b. Minimum password length = 8 characters
c. Password must meet complexity requirements = containing a mix of numbers, letters and symbols
d. Where available 2fa (two factor authentication) must be used
e. Password must not be shared with other people or used in 3rd party systems

Anti-Virus and Cyber Security

a. Anti-Virus software should be installed on all PDNPA computers and mobile devices. Report to IT Support if you suspect it is not working or is missing
b. If you are notified about a virus on your computer, turn it off and contact IT Support
c. Ensure websites, e-mails, links and attachments are genuine before opening
    a. If in doubt = do not click

Social Engineering

Social engineering is a term to describe "*Manipulating people into carrying out specific actions, or divulging information, that's of use to an attacker*"

Summary of your responsibilities

a. Challenge and ask for ID.
b. Be sure you know who you are talking to

Clear Desk Policy

Purpose - to reduce the risk of a security or data breach, fraud and information theft. Ensure we are compliant with data protection regulations by demonstrating that we are taking responsibility for the personal data we collect and storing it securely.

Summary of your responsibilities

a. Ensure your desk is clear of files (electronic and paper)
b. PDNPA equipment (laptop, phone, tablet etc..) is taken home or secured in a locked drawer
c. Drawers and filing cabinets are locked overnight
d. Papers containing personal or confidential information should be shredded or deposited in the confidential waste bins

Section 2 Acceptable Use and ICT monitoring

Purpose – staff adopt the rules for use of assets associated with information processing and how the use is monitored

Summary of your responsibilities

a. Manage your mailbox and check your mail regularly
    a. Storage limits are set and outbound email blocked when the limit is reached
b. Keep your calendar updated with your location
    a. Out of office should be used when you are away from the office for any length of time, for example on holiday
c. Make yourself available for telephone calls
d. When available web cameras must be used during online meetings
e. Email addresses are sensitive data
    a. Use 'mail merge' for multiple recipients
    b. Check the recipient address before sending
f. Use links rather than attachments where practical in messages
g. Freedom of Information
    a. Emails may be shared beyond their intended audience
    b. Take care not to express unprofessional views
h. Licensing – TV and Broadcast
    a. A TV license is required to listen or watch broadcast content online e.g. BBC Radio or a TV program
    b. Headphones must be used – we do not hold the appropriate commercial licenses to broadcast
    c. Work use only
i. Personal use of social network sites and video interactive sites (e.g. YouTube) are not permitted
j. Software use must be legal and compliant with FAST (Federation against software theft)
k. Online content and services should meet accessibility standards
    a. Understanding WCAG 2.1 - Service Manual - GOV.UK (www.gov.uk)

ICT Reporting and Monitoring Summary

Summary.pdf

Document contents:

U drive quota
K drive routine deletion
Monitoring of email and internet use
Network access control
Server backup and archive
Auditing and management software on our computers

Inappropriate material, if found, will be reported to the police.

Section 3 Data & records management:

Purpose – good records management supports good data governance and ensures compliance with data protection, making sure that staff can find the information they need to support decision-making and enabling more effective use of resources.

Summary of your responsibilities

a. check there is only one master copy of data that has a named owner and is registered in Informu
b. limit permissions for editing or deleting data to those who need it
c. ensure the security of personal and confidential data
d. ensure that personal or subjective comments can be substantiated
e. check that your data is valid
    a. correct any inconsistencies
f. meet our commitment to transparency and public accountability
    a. evidence our activities or decisions
g. ensure the application of our records retention policy
    a. actively manage the data you hold and dispose of it when it is no longer required.
    b. records that have been identified for disposal should be destroyed in an appropriate manner
    c. electronic storage devices should be passed to IT Support for destruction and disposal
h. demonstrate, compliance with the GDPR principles for processing personal data
    a. obtain and process data fairly and lawfully and in a transparent manner
    b. collect data for specified, explicit and legitimate purposes
    c. ensure the data collected is adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed
    d. ensure that the data is accurate and where possible, kept up to date
    e. data is processed in a manner that ensures appropriate security
i. Be aware of the rights an individual has in regards to our processing of their data, including making a Subject Access Request (SAR).
j. Particular care should be taken when processing special category data (such as health information)
    a. disclosure normally requires the explicit consent of the data subject
k. processing FOI and EIR requests
    a. 20 working days in which to respond
    b. if clarification is needed, the 20-day deadline starts from the date the additional information is received
    c. respond to the request in the format specified

d. inform applicants of their right to appeal if any of their request is refused because of an exemption
e. it is a criminal offence to destroy or dispose of records once a request has been received

Ensuring our data is of the highest quality and meets relevant legal requirements

Guidance and Policy documents (Folder Link):

Folder Contents:

Data Protection Policy
Privacy Notices
Breach Notification Process
Clear Desk Guidance
Controllers, Processors and data sharing
Managing Consent
Subject Access Request
Data Protection Impact Assessment
Retention guidance and schedule
Leavers records Management Procedure
Information Management Strategy

Records Management

Electronic filing guidance
Managing paper records

Draft Guidance is available upon request from the Records Manager

Our Publication Scheme: Web link to FOI information on Peak District website

Accessibility Statement: Web link to the statement on Peak District website

For clarification or further information speak with your teams Information Asset Owner (IAO) or the Authorities Records Manager

Section 4 Advice and Guidance

Further advise and guidance is available from: Folder Link

Folder Contents:

- Starting and Leaving the PDNPA
- Accessible PDF documents
- Social Media guidance
- Microsoft Teams, Chat, Video and collaboration tools
- Services from 3rd party websites – Security and Guidance
- Managing Email
- Procurement and disposal
- Hardware and Software Standards
- CCTV Code of Practice
- Equality Impact Assessment Guidance
- IPR and Copyright Law.
- guidance on the use of images & photographers rights
- ICT Blended Working Principles

In addition, if you have access to SysAid the IT Helpdesk system.
There is a Knowledge Base with regular updates to the FAQ's section.

Appendix 2 details the ICT support service: how to request advice, guidance, report an ICT issue or request support.

Appendix 1

Information Management Strategy Principles:

Vision of how we will be when the strategy is fully implemented:

1. All information will be managed electronically (including post and staff calendars). Paper files will be used for archive purposes and you should think carefully about the need to print documents (e.g. when consultees have no way of viewing electronic documents or staff need to take large format documents on site).

2. Data will be restricted to a single source (one working copy of each document or dataset) that can be shared easily with others (e.g. automatically made available to partners or the public using document management software and the internet).

3. Rights (to create, read, edit, write or delete data) will be controlled by the Information Asset Owners (IAO) who are responsible for ensuring the accuracy, relevance and security of the data.

4. Infrastructure (servers, PCs, etc. and the network that joins them together) and information systems (software programs) will be sustainable and delivered to industry standards. They will be procured and developed corporately (and where appropriate, jointly with other National Parks) to integrate with existing technologies wherever possible.

5. Voice/video/data will be available to all desktops (including remote centres, home workers and members) via a high speed, dependable network or secure (VPN) broadband.

6. Secure mobile computing will be available for managers and field staff. It will be easy to use and integrate with office based systems.

7. A single set of IT policies and operating standards will be adopted by all staff to improve security, training and support, and to simplify system maintenance.

8. Easy to use, web based interfaces and services will be developed wherever possible. Where not possible, consideration will be given to how users, including remote users, will access information and services.

9. Staff will be trained and supported in using systems by an adequately resourced core IT staff that will be responsible for maintenance of the infrastructure. Technology will be used to reduce our carbon footprint.

Appendix 2

IT service level agreement (SLA)

Background

There is a team of 3 IT Support Officers, who look after the network, telephones, Infrastructure, end user equipment and software.
Specialist management and support is provided by 5 offices (4fte) in the areas of; GIS, web & online services, database (inc. business systems) and records management.

As well as dealing with day to day enquiries the team work on improving the overall standard of IT provision in accordance with the principles set out in the Information Management Strategy and the Digital Plan.

Your responsibilities

Before contacting IT Support, please try and find a solution to the problem using frequently asked questions in SysAid or by checking with colleagues.

If you cannot find a solution, raise a support request through SysAid

If SysAid is unavailable;
email or call PDNPA IT Support

Support requests should be prioritised using the following guide criteria:

- high –urgent cases where you are working to an immediate deadline and where no workaround is available, or the problem is affecting a greater number of people
- normal – where a problem is preventing you continuing a specific task but a workaround is available and/or you have other tasks you can work on
- low - for non-urgent support or requests on tasks that do not immediately affect your work
- project – for all new and developmental work

Please be realistic in your expectations as the team is small and deals with a variety of calls and manages a number of projects.

Please ensure you provide as much detail about the problem as possible. The SysAid support request form is set up to help you do this. The more detail you provide, the greater the chance the problem can be solved promptly.

Don't expect preferential treatment if you drop into the IT Office. To manage the volume of work and provide a fair service to all, requests will be processed using SysAid.

Accessing IT Support

The support desk is available from 09:00 to 16:00, Monday – Friday.

Calls raised through SysAid are acknowledged automatically with emails sent as the ticket is updated.

Requests made by phone and email will be entered into SysAid, we will request that you do this asap. When the team is very busy this may result in a delay in dealing with your request.

IT Support reserve the right to review priorities for consistency and equity across the Authority.

Network and other issues affecting many people will normally take priority over support requests where one or a small group of people are affected.

Remote support

IT are able to provide remote support to PDNPA devices and mobiles.
Remote access is obtained via a 3rd party support tool with PDNPA branding.
The prerequisite for support is a suitable internet connect with access to the internet to open the support link on the device with the issue.

We make site visits to PDNPA offices.
We may ask you to bring equipment to Aldern House, Bakewell.
We do not, under any circumstances, visit private residences or support non-PDNPA hardware.

Exception to password policy for IT Support

There may be circumstances when IT Support need to log into a computer or system with your user account to troubleshoot or fix an issue specific to you. In these circumstances you may share your password with IT Support or, having sought your permission, they will change the password to allow themselves the access they require.

Upon resolution of the issue, you should change your password so that it is only known to you.

Appendix 3

Completing the **Information Management Policies Framework computer users' agreement form** is a prerequisite for access to the PDNPA's IT services such as computers, email and server or data access.

Failure to complete compulsory ICT training within agreed timeframes will result in the removal of access to PDNPA ICT services.

Training is provided via an online platform independent of PDNPA ICT systems