Lake District National Park Authority
Complete ICT Policy Framework

V2.0 2/9/2025, next review 2/9/2028 or sooner.

Version 1.0 27/7/2017

Version 1.1 amended to link to data retention policies 21/8/2018

Version 1.2 amended to include firewall, antivirus and Information Security Incident Management policies (Sections 18, 19 and 20) 27/11/2018. Changes to Password requirements sec 12

Version 1.3 amended to clarify use of smartphones – personal data on Authority phones and Authority data on personal phones and updated legislative references

Version 1.4 17/12/2021 Minor amendments to reflect changes in systems (Replacement of Citrix, Addition of MS 365), email spoofing tests

Version 2.0 Splits policies in two Corporate (Backup, security etc) and end user

This document provides a full summary of all ICT policies for the Lake District National Park Authority and will be referred to by the ICT team when implementing any requests or changes.

Policies in this document may affect ICT infrastructure and/or end users. A summary of policies directly applicable to end user behaviour is published separately.

Contents

See also Data Protection Policies (Legal Team)

1. Account Management

Summary

Your user account grants access privileges to LDNPA ICT systems and services. All users of ICT systems will only be provided with the privileges that they need to do their job. Accounts will be reviewed every 3 months to ensure that passwords are being changed in accordance with this policy and leaver's accounts are disabled or deleted as appropriate.

This Policy governs:

- The creation, management and deletion of user accounts
- The granting and revocation of authorised privileges associated with a user-account
- The authentication (usually a secret password) by which the user establishes their right to use the account

Account Creation

Except for service (non-user specific) accounts, Domain user accounts will only be created on receipt of a new user request form, signed as appropriate and passed to the ICT team from the HR team

Account details will only be handed to the user concerned after completion of the ICT essential training session; this will usually be conducted in person but, in exceptional circumstances, may be completed remotely through teams/telephone.

Once a user has completed this initial training, they will be supervised by ICT staff in initial logon to the domain and setting their own password.

Account usage will be monitored including date, time and approximate location of sign-in

Account Deletion

Upon notification from the HR team by way of a completed leaver form, the relevant user account will be disabled at the agreed data and time, typically the end of the users last working day. This will deny access to all systems including remote systems.

Any LDNPA equipment such as mobile phone and laptop is to have been returned by this time.

The email inbox and OneDrive data for the leaver will be made available to the line manager for 30 days.

The leavers account will finally be deleted after 30 days **Access Control**

The creation, deletion and changes of user accounts and privileges must be carried out by trained and authorised staff.
The person enacting any change in a user account must be different from the one authorising/requesting the change.
Account details will only be divulged to the user after proof of identity has been established.
Accounts will be reviewed regularly to ensure obsolete accounts are removed or disabled

Managing Privileges

A user account should have the least privilege which is sufficient for the user to perform their role within the Authority.
Changes in the privilege of an account must be authorised by a nominated “owner” of the system to which the account affects.
Procedures shall be established to ensure that users’ access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, a user changes their role, or a user leaves the Authority.

Monitoring

Accounts will be reviewed regularly according to the Account review Procedure.
Accounts unused for a period of 2 months will be deleted unless an exemption applies such as maternity or other long term absence

2. Data Management and Retention

The Authority does not operate a separate archiving system. It is the responsibility of each user to maintain any data relevant to their role which needs to be retained.

Decisions on retention should be made with reference to the Data Retention and Information Management Policy

Data is backed up for business continuity, currently 3 months of backups are retained

Use of external storage media – hard drives, Memory sticks, SD cards etc is no longer permitted for data storage and cannot be saved to.

An exemption may be granted where a third party requires the use of data on such a device.

Data can still be accessed on such devices if received from third parties, but electronic file sharing (OneDrive etc) is preferred.

3. Asset Management

Summary

This policy refers to ICT assets defined as but not limited to:

- Fixed computer equipment, e.g. servers, desktop computers;
- Portable computer equipment, e.g. laptops, mobile phones, tablets;
- Processing peripherals, e.g. printers, photocopiers;
- Storage Media, e.g. hard drives, USB storage devices, network attached storage;
- Software, e.g. desktop business applications, operating system, administration software;
- Databases and data stores;
- Audio Visual equipment, e.g. projectors, smart boards, controls systems;
- Network infrastructure, e.g. routers, cabling, telecommunications;
- Data centres, server rooms and supporting infrastructure, e.g. security systems, air conditioners, generators.

ICT hardware assets will be monitored and audited. Under-used assets will be recovered by ICT and deployed elsewhere.

Policy

Asset procurement must be agreed in advance with the ICT Services Manager and reflect the needs of the user(s). Replacement of end-of-life assets will be built into ICT budgets as part of the finance planning process.

ICT hardware and software assets required for specific projects or outside the general asset replacement must be included in project budgets. This includes any revenue costs incurred up to the next financial year, where, if agreed, maintenance will be added to the ICT budgets.

Management

All Authority computers will be managed and monitored through Microsoft Intune management which enables bulk remote management and monitoring of devices

Software assets will be monitored to ensure compliance with licencing requirements.

Hardware assets which have not been active for a period of a month will be reviewed by ICT with the relevant line manager and redeployed if necessary.

Security

Only Authority domain joined PCs may be connected to the Authority network at any site.

All assets are to be protected by a password or PIN as appropriate. Laptops and tablets and other portable storage will be encrypted with keys to be held by the ICT team.

Protection

Each user must protect and use assets with appropriate care. Portable assets should be secured when unattended.

Loss or theft of any asset should be reported to the ICT team as soon as possible.

Loss of any device containing data must also be reported to Legal services, this includes smart phones containing email, chat and similar information.

Disposal

Disposal of any asset which contained data including, but not limited to hard drives and tape media will be carried out according to the Waste Electrical and Electronic Equipment regulations (WEEE) regulations and a certificate of secure erasure for each device is to be obtained.

CDs and DVDs will be shredded onsite.

4. Electronic Security, Data Backup and Recovery Policy Statement

Summary

Purpose and Scope

To summarise the Authority's Policy on protection of electronic data

Context

The LDNPA ICT Service and suppliers will ensure secure storage and backup of any data stored on its servers. Data backed up will be copied offsite daily to mitigate fire risk and retained for three months. Users should ensure data on PCs is synchronised through OneDrive. It is the responsibility of everyone to ensure required data is stored in a secure location.

The primary purpose of a backup is to recover systems in the event of total loss or other disasters.

5. Change Control

Change Management Policy

Introduction

The purpose of this policy is to document the way that we manage changes that occur to the ICT Service. This will be done in a way that minimises risk and impact to the Authority. It will also define a Change as understood by ICT and to describe the accepted Interim Change Management procedure.

Definition of a change

For the purposes of this document, a change will be defined as anything that transforms, alters, or modifies the operating environment or standard operating procedures of any system or service that has the potential to affect the stability and reliability of the infrastructure or disrupt the business of the Authority.

Changes may be required for many reasons, including, but not limited to:

- User requests
- Vendor recommended/required changes
- Changes in regulations
- Hardware and/or software upgrades
- Hardware or software failures
- Changes or modifications to the infrastructure
- Environmental changes (electrical, air conditioning, data centre, etc)
- Unforeseen events
- Periodic Maintenance

Policy

It is the responsibility of the ICT Service to manage the life cycle of all the systems supporting the Authority´s business and technical objectives. As such, all the processes and procedures relating to change control and management are set out in the document "Change Management Procedure".

Changes are categorised as follows:

1. Minor/Routine (system patches and service packs)
2. Emergency/Unscheduled – Change to restore services
3. Major/Significant (Software version or hardware upgrades)
4. New Development.

For any change above level 2, the following conditions must be in place.

- A documented plan of the sequence or steps for implementing and releasing the change into the live environment. This should be stored in an appropriate place e.g. shared drive.

- Where possible, evidence demonstrating the fact that this change has been tested in a pre-live/staging environment first.
- A rollback/mitigation plan in case of failure.
- A post-change test being documented to check that the change has been successfully applied.

Incidents

Where a change has caused an incident, a review meeting and a report will be generated and fed back to the ICT Services Manager

Scope

The scope of the Change Management Policy and the procedures contained within it are applicable to all members of The ICT Service and its authorised colleagues and are related to the management of changes to all the ICT Service managed live IT systems or services.

Exclusions

The Change Control system is not for customers to request changes or enhancements to any service or system, rather it covers items such as major patches and configuration changes to back-office systems and servers.
Changes and enhancements to ICT applications and hardware can be made directly to the ICT Services Manager or through user forums.

Risk

By actively planning and managing changes for the benefit of users, we should be able to deliver a better and more reliable experience to our customers; this should be done in line with the Authority´s business needs. If not properly controlled, changes could be made which will have a negative impact on the Authority and could prevent people from fulfilling their roles. Changes could also be made by individuals who are not fully aware of the impact on other areas of the Authority. All changes should undergo a risk assessment to determine the probability of it occurring and the impact it would have on the Authority.

Roles and Responsibilities

The ICT Services Manager ensures that changes follow the Change Management Procedure and will review the policy to ensure that it is up to date and relevant.

Everyone in the ICT Service has a potential role and corresponding responsibility with regards to Change Management.

End-Users/Functional Teams:

1. Submitting enhancement requests through the appropriate systems

2. Participating in testing, pre-deployment testing and post deployment testing
3. Timely sign off for the change
4. Verifying that change requests are valid
5. Computer Use

6. Information Security

Purpose and Scope

The information stored in manual and electronic systems used by ICT Users represents an extremely valuable asset. The increasing reliance on ICT for service delivery makes it essential to ensure that these systems are developed, operated, used and maintained in a safe and secure fashion.
The purpose of the Policy is to ensure the confidentiality, integrity and availability of the Authority's information is maintained by implementing best practice to minimise information risk.

Applicable To

- All ICT Users.
- All physical locations from which Authority systems are accessible
- Any device capable of storing data electronically
- Paper records
- Any other media

Intention

The intention of this policy is to ensure that all ICT Users understand their individual responsibilities in relation to the Authority's electronic information systems such that:

- Regulatory and legislative requirements are met.
- Authority information is protected against unauthorised access.
- Confidentiality of information is assured.
- Integrity of information is maintained.
- Business requirements for the availability of information are met.

Context

Some aspects of information security are governed by legislation; the most notable United Kingdom Acts are:

- The Data Protection Act (2018)
- Copyright, Designs and Patents Act (1988)
- Computer Misuse Act (1990)
- Regulation of Investigatory Powers Act (2000)

- Freedom of Information Act (2000)
- Environmental Information Regulations (2004)
- Human Rights Act (1998)
- Equalities Act (2010)
- EU General Data Protection Regulations (2018) (Principles incorporated into UK legislation since Brexit
- Data (Use and Access) Act 2025

ICT Responsibilities

- Provide induction training to all ICT Users to ensure they have a proper awareness and concern for computer system security and an adequate appreciation of their responsibility for information security.
- Design, implement and maintain suitable network security and infrastructure to protect the Authority's information from unauthorised access
- Ensure all computers are running appropriate active and current Antivirus software, and software security patching is up to date
- Maintain the availability of ICT hardware, software and systems and the information they contain
- Block portable devices
- Periodically check that all staff have the skills necessary to detect and manage malicious email and provide training as needed
- Implement systems to monitor for personal and other sensitive data leaving Authority systems

7. Network Monitoring

Purpose and Scope

The purpose of network monitoring is to identify and block malicious activity and performance issues in order to protect and optimise the Authority's data, systems, and reputation.

Applicable to

All computing systems and network infrastructure owned or managed by the Authority.

Intention

To ensure the protection of ICT systems and data, pre-empt malicious activity and ensure systems are running reliably and securely

Context

In order to protect data, ICT staff may use network monitoring technologies to log network activity and to scan data moving across the network. These technologies may include:

- Anti-virus software
- Email filtering
- Web filtering
- Firewalls
- Intrusion protection and intrusion detection
- Vulnerability assessments
- Database and application monitoring systems
- Monitoring of server and PC logs

This information may be centrally correlated for analysis.

Server logs are generated automatically and can be monitored for troubleshooting. Network traffic from offices or on VPN is classified by destination and retained for 30 days for troubleshooting and resolution of network issues. These measures are not generally used for tracking and/or monitoring an individual's network activity. Confidentiality of all information gathered as a result of network monitoring will be maintained at all times. Access to information obtained through network monitoring will be limited to designated staff and in the event of an investigation, Authority officials, legal counsel, or law enforcement. This information will be kept in a protected storage area.

Any substantive changes to the network monitoring methodology or scope must be approved by the Authority's senior management. In addition, key network sites will be monitored to determine system availability

8. Password Management

User passwords are the key method of access to the LDNPA systems

- User passwords will expire every 180 days and must be changed at that time
- Passwords must be a minimum of 10 characters in length
- User passwords must not be divulged, shared or in any other way compromised
- Password changes are enforced, the same password cannot be reused

Policy

A user ID and password are required to gain access to all LDNPA ICT systems.

Password must meet the following requirements:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least ten characters in length
- Contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example: !, $, #, %)

Your ID and password will be the same for most systems and passed through automatically in most cases. More sensitive systems, for example, Finance and Planning will have separate passwords in addition to network logon

Passwords will expire and need to be changed every 180 days. A new password will be required and cannot match any of the user’s previous 10 passwords

Once changed, a password cannot be changed for the next 24 hours

Incorrect entry of a password 3 times will lock out the user account for the next two hours

If a system is being used which does not support changing passwords, ICT may grant an exception to the 180-day rule. Such systems include:

- Remote only users (e.g. Members)

9. Patch Management

Summary

The Authority operates an extensive number of Microsoft Windows systems, both desktop PCs and Servers. It is essential that these systems are kept up to date, ensuring the latest updates are deployed. This will ensure that systems are reliable and all known security vulnerabilities are patched.

Users should install updates as soon as they are notified they are available

Policy

All Authority Servers, Desktop, Laptops and windows Tablets are configured through group policy to obtain updates directly from Microsoft.

Updates will be downloaded daily and deployed weekly in accordance with Microsoft general policy.

Updates will be released to users 1 week after publication, in this way, any updates which may adversely affect operations can be detected before a widespread event can occur.

Should a major issue be announced by Microsoft and an emergency patch released, this will be deployed immediately.

Updates will be installed automatically but users are encouraged to ensure they are installed as soon as possible and, where necessary, systems restarted.

Some key systems which cannot be allowed to restart automatically will be patched manually out of hours by datacentre staff, for example, mail server and backup servers.

ICT staff will monitor systems on a monthly basis, any Desktop PC which has not made contact with the update server for over a month will be checked to ensure the update services are functioning correctly and any issues resolved. Any system which proves to have been unused for a month or more may be recovered by ICT as surplus to requirements after discussion with the relevant manager. Any mobile system which has not made network contact will be recalled by ICT for be checked and patched accordingly.

The above policy does not cover anti-virus updates which are deployed to all systems automatically as released by the provider.

Other Systems

Meraki firewalls are updated automatically through the Meraki cloud. Other systems are monitored and updated manually or as notified by the service provider.

10. Privileged Access

Summary

This policy applies to any user with access to a domain account in any of the following Active Directory Domain groups or access to the Domain Administrator account

Server Operator

Account Operator

Domain Admin

Enterprise Admin

Schema Admin

Any user of an account with any of the above privileges is subject to extra constraints over and above the standard user acceptance term with which they must also comply

Detail

Any user requiring access to any of the above listed privileges will be issued with a second user account.

The second account will not be issued with an email inbox.

In day-to-day work, it is expected that the user will log on and use their standard domain account.

Use of the privileged account will be only on an as-needed basis, for example:

- Connecting to a server for the purpose of configuration or other maintenance
- Running RSAT (Remote Server Administration Tools) consoles from the users own device
- Elevating access to systems when using a standard account

It is expected that once any such work is completed, a user will log off, close or otherwise secure the device running privileged permissions.

Note, final testing of systems should be conducted with standard user permissions

Any changes made using privileged access should be logged in the Change control log

Privileged Access will only be granted on completion of a Privileged Access user form

Privileged access group membership will be reviewed on a quarterly basis as described in the Account Management Policy and Procedure.

Privileged Access can only be granted by the ICT Services Manager.

Request for Privilege Access account

Name

Job title

User Name

Access required

Group	Required
Server Operator	
Account Operator	
Domain Admin	
Enterprise Admin	
Schema Admin	

Reason for Access

Authorised by

ICT Services Manager

Date

11. Secure data transmission

Purpose and Scope

This policy concerns transmission of sensitive or personal data as described in the Information Asset Register to third parties and organisations either electronically or using media such as CDs, DVDs and USB Memory Sticks

It is expected that data transmission will now use the tools provided in Microsoft 365 (Onedrive/Teams/Sharepoint) and that these tools will replace the systems described above

Applicable to

All users responsible for sharing data as described above

Intention

To ensure the protection of stored data, safe transmission of data

Context

Data can be shared in a number of ways as described above, the Authority and staff has a responsibility to secure any personal and sensitive data.

- Any such data transmitted electronically over public networks including the internet must be encrypted, this is commonly achieved using a dedicated application or SSL encrypted website or secure transfer application
- External storage media cannot be written to (read only) unless exemption is granted by ICT Services Manager (for support of certain systems)
- Cds and DVDs are not to be used for sensitive or personal data due to limitations on encryption.
- Email encryption is supported by default, mail delivery will fail if encryption is not supported by the receiving party (MTA-STS)
- Any folder containing personal data will be registered on the Information Asset Register and have suitable security restriction
- Any information shared with other organisations must be registered in the Information Asset Register

12. Systems and Network Security

Purpose and Scope

This policy describes the processes in place to protect ICT systems physically and electronically

Intention

To ensure understanding of ICT security

Context

ICT systems have a number of vulnerabilities, these can include the following

- Physical access to servers
- Access to servers and other systems through the internal network
- Wireless access to the network
- Access to systems through end points such as PCs
- Access to systems over the internet
- Fire risk

Policy

Physical access to servers

Servers and other back office systems will be located in secure rooms with suitable environmental control. Access to server rooms will be restricted by door PIN codes which will be made available only to key staff (Server room register). PIN codes will be reviewed annually or after the departure of a member of staff. No PIN holder may divulge the PIN to another user. Server rooms are monitored for temperature and overheating is notified to the ICT team by email and SMS text.

Should server room overheating not be attended to, servers will shut down automatically

Access to servers and other systems through the internal network

Network points can provide direct access to system. This is especially a risk where live data points are located in public areas. It is therefore policy that no data point will be enabled in any area which may host events or other meetings attended by members of the public. If corporate network access is required in these areas, it will be either wireless or by special request for a limited period to the ICT services Manager.

Wireless access to the network

Wireless access to the Authority network is protected by RADIUS security. Only windows PCs which are part of the LDNPA domain can join the corporate network directly.

Non-windows machines inside the Authority are treated as external.

Access to systems through end points such as PCs

PCs and other devices provide direct access to LDNPA systems. Only LDNPA owned machines as configured and approved by the ICT service may be physically connected to the corporate network.

No third party or guest system of any type may be joined to the Authority network.

Users must consult with ICT where new hardware is required, not all systems are compatible with corporate networks, for example, Windows Home editions will not connect to corporate services.

Access to systems over the internet

LDNPA Datacentre has a limited number of systems exposed to the internet, this number is deliberately kept to a minimum to reduce risk to corporate systems. The Authorities Web presence is hosted elsewhere and new web services should not be deployed on the existing web solution.

The Authority firewalls protect each site and are automatically updated for firmware and malware definitions.

Monthly tests are conducted to determine any weaknesses in firewalls and for sites which need PCI compliance, a quarterly test is conducted

Private/public segregation

There will be segregation of networks, either physically or by firewall, specifically:

- Corporate LAN
- Public Access
- PCI Card Data Environment (See separate PCI documentation)

Any unused network ports will be disconnected

Corporate network ports must not be enabled in public areas

Wireless security will be the latest available version (WPA3) for all networks

13. Third Party Code of Connection

Purpose and Scope

This policy recognises the need for third parties to connect to LDNPA systems where an exception to section 12? (Above) applies. Exceptions are listed below.

Applicable to

Any and all third parties, suppliers and support staff

Intention

To ensure understanding of ICT security

Context

A number of systems will from time to time require support from providers or suppliers. This support may be in the form of remote access or on-site assistance. It may be necessary for a technician to connect directly to systems across the corporate network using a non-authority machine

Policy

- Any third party organisation needing to connect to LDNPA systems must be on the list of approved organisations managed by the ICT Services Manager
- The list of approved organisations will also list the way they can connect to LDNPA systems
- Access is granted on a basis of minimum rights necessary to perform the task in hand
- A dedicated AD account will be created as needed for use by third party. This account is to be disabled by ICT staff when not in use
- Organisations and their representatives must be supervised by a member of LDNPA staff at all times

14. Firewall Configuration and Maintenance

Purpose and Scope

This policy covers the management of LDNPA firewalls including access, rule configuration, sign-off and firmware management. It is complemented by the firewall procedure and schedule document.

Applicable to

ICT staff as listed in the Firewall procedure and schedule document.

Intention

To ensure firewall operation and management is understood, secure and robust

Context

The Authority operates a firewall at each internet facing site, these firewalls protect each site from hacking and malware. At most sites, they also provide our connectivity to HQ through VPN.

It is essential that each member of staff authorised understands their role in the management of these devices to maintain a secure perimeter

Cisco ASA firewalls at datacentre protect internet facing servers and are maintained and patched by Iomart. ICT services manager can request changes to these devices

Policy

- Any firewall accessible or managed from a cloud console must be secured by two factor authentication
- Firewall administrators must be approved by the ICT Services Manager, this would usually be restricted to ICT Services Manager, Helpdesk technician, Systems Analyst and developer roles
- Read only access may be granted on Meraki devices for non-ICT staff to access location analytical data
- Any rule changes must be cleared with the ICT Services manager prior to implementation, if unavailable, direct instructions from firewall supplier or listed third party support provider may be implemented
- Any changes to firewall configuration must be recorded in the Change Log
- Firewall firmware must be kept up to date, firmware versions should be reviewed on a monthly basis
- Firewall security must be tested on a monthly basis through and external vulnerability assessment
- Firewalls at sites handling card payments must pass a quarterly PCI DSS scan in addition to the above

- Any vulnerabilities rated high must be addressed within a week or added to the Risk Impact Assessment log. Any other vulnerabilities should be addressed within a month or added to the ICT risk register
- Outgoing rules will be generally open with the exception of port 25
- Incoming rules will be restricted to required NAT only, for example web servers and telephony
- Firewall will be maintained between all VLANs to prevent VLAN hopping
- Meraki Advanced licenced systems must have AMP malware protection enabled

15. Antivirus Configuration and Maintenance

Purpose and Scope

This policy covers the management of LDNPA antivirus solution including access, rule configuration, sign-off and update management.

Applicable to

ICT staff as listed in the Antivirus procedure and schedule document.

Intention

To ensure Antivirus operation and management is understood, secure and robust

Context

The Authority operates Microsoft Defender, this covers Windows desktop PCs and tablets, servers and MS Exchange. There is a web proxy virtual appliance which monitors internet traffic for malware and logs usage.

Mail traffic is in addition supplemented by Vipre and MS Defender which scans incoming and outgoing mail for malware as well as providing spam detection.

It is essential that each member of staff authorised understands their role in the management of these services devices to maintain a secure perimeter

Policy

- Microsoft Defender must be enabled on each endpoint (PC, Tablet or server).
- Antivirus will be monitored daily from the Microsoft Security Portal by the helpdesk team to ensure that machines are compliant
- Incidents of virus or malware must be dealt with according to the Incident and Response Plan

16. Information Security Incident Management Policy

See also

Data Protection Policy

Purpose and Scope

The Authority is responsible for the security and integrity of all data it holds and must protect this data using all means necessary, ensuring that the risk of any incident which could cause damage to the Authority assets and reputation is prevented and/or minimised.

Applicable to

This Policy applies to all Services, Partners, Employees and Members of the Authority, contractual third parties, Committees who use IT facilities and equipment, or have access to, or custody of, customer information or corporate information.
All users have a role to play and a contribution to make to the safe and secure use of technology and the information that it holds.

Intention

To ensure clear understanding of the nature of an information security incident and explain the necessary actions should an incident occur.

Context

A security event is an identified occurrence of a system, service or network indicating a possible breach or failure of safeguards, or a single or series of unwanted or unexpected events have a significant probability of comprising the business and its information security.

Incidents may include:

- loss of confidentiality of information in any format
- compromise of integrity of information
- denial of service
- unauthorised access to systems
- misuse of systems or information
- theft and damage to systems
- virus attacks
- Computer left unlocked with access to sensitive data
- Unsupervised or unauthorised individuals in non-public areas
- Cabinets or rooms containing sensitive data left unsecured

Other incidents may include:

- Missing correspondence
- Exposure of Uncollected printouts
- Misplaced or missing media
- Inadvertently relaying passwords

- Loss of mobile phones and portable devices including laptops, tablets and memory sticks

This policy needs to be applied as soon as information systems or data are suspected to be or are actually affected by an adverse event which is likely to lead to a security incident as outlined in the above list.

The Authority will take steps to identify and mitigate risks to data, this will be recorded in the Risk Impact Assessment log.

Policy

This policy is designed to ensure the Authority meets its Statuary duty in the case of a data breach, including notifying the correct Authorities where appropriate, taking steps to mitigate the breach and prevent any repeat.

Any individual discovering a security incident must in the first instance report it their line manager and then to the ICT Helpdesk and Data Protection Officer using the Data Security Breach Reporting form

Where appropriate, the ICT team will invoke the appropriate Incident response plan(s)

17. Cyber Security Policy

Lake District National Park Authority

17.1 Introduction

This policy outlines the cybersecurity practices and responsibilities required to protect the digital assets, data, and ICT systems of the Lake District National Park Authority. This document is designed to comply with UK data protection laws, including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

17.2 Purpose

The purpose of this policy is to:

- Protect sensitive data, including the public's personal data and our own information.
- Ensure the confidentiality, integrity, and availability of digital systems.
- Mitigate cybersecurity risks and ensure compliance with relevant legal and regulatory frameworks.
- Promote awareness among staff about cybersecurity risks and best practices.

17.3 Scope

This policy applies to all employees, contractors, volunteers, and third parties who access or use the ICT systems, network, or data of the Lake District National Park Authority.

17.4 Key Cybersecurity Risks

The following risks have been identified as critical to the security of the Lake District National Park Authority's systems and data:

- Phishing attacks: Unsolicited emails or links intended to compromise login credentials or deliver malicious software.
- Malware and ransomware: Malicious software designed to damage or disrupt systems or hold data hostage for ransom.
- Unauthorized access: Attempts by malicious individuals to gain access to systems or data without permission.
- Insider threats: Unintentional or deliberate misuse of access to data and systems by employees or contractors.
- Data breaches: Unintentional exposure of sensitive or personal data due to vulnerabilities or attacks.
- Weak passwords: The use of weak or compromised passwords can allow unauthorised access.

- Unpatched software and systems: Outdated software and systems may have vulnerabilities that can be exploited by attackers.

17.5 Roles and Responsibilities

17.5.1 Senior Management

- Ensure compliance with this policy and UK legal standards.
- Oversee the allocation of resources necessary to maintain effective cybersecurity practices.
- Approve and review this policy on an annual basis.

17.5.2 ICT Department

- Implement technical controls to secure the ICT infrastructure (firewalls, anti-virus software, encryption, etc.).
- Monitor and respond to any cybersecurity incidents.
- Ensure systems and software are regularly updated and patched.
- Enforce multi-factor authentication (MFA) for all accounts.
- Maintain regular backups of critical data and ensure disaster recovery plans are in place.

17.5.3 Department Heads

- Ensure staff are aware of this policy and adhere to its guidelines.
- Work closely with the ICT department to identify and mitigate potential cybersecurity risks in their departments.

17.5.4 All Employees

- Adhere to cybersecurity best practices, including regular password changes, avoiding phishing emails, and reporting any suspicious activity.
- Comply with restrictions on personal use of government ICT systems.
- Participate in mandatory cybersecurity training programs.

17.5.5 Third Parties and Contractors

- Ensure they follow the same cybersecurity guidelines and standards as employees.
- Provide evidence of their own cybersecurity measures where applicable.
- Report any cybersecurity incidents that could affect the authority's systems immediately.

17.6 Security Controls and Measures

17.6.1 Access Control

- Role-based access control will be implemented, ensuring that employees only have access to data and systems necessary for their role.
- Staff must use strong, unique passwords for all accounts and adhere to a password policy requiring changes every 180 days.
- All accounts must use MFA.

7.6.2 Data Protection

- All data must be encrypted at rest on mobile devices and in transit, following GDPR requirements.
- Access to sensitive data must be logged and audited regularly using the Information Asset Register
- Staff should minimise the amount of personal/sensitive data stored locally on devices and ensure sensitive data is stored on secure, approved cloud services.

17.6.3 Email and Internet Use

- Staff, Members and volunteers are prohibited from using personal email accounts to conduct government business.
- Use of the internet for non-work-related purposes is permitted during breaks but should be minimal and not violate security policies.
- External email attachments from unknown sources should not be opened without ICT approval.

17.6.4 Device Security

- All devices accessing the Lake District National Park Authority systems must be approved and secured using authority-approved security software.
- Employees must ensure their devices are physically secure, and remote access must be conducted via secure Virtual Private Network (VPN) connection (Cisco AnyConnect).
- Lost or stolen devices must be reported immediately to the ICT department and Legal Services.

17.6.5 Incident Response

- Any cybersecurity incident must be reported immediately to ICT.
- ICT will investigate and respond to incidents in accordance with the incident response plan, including containment, eradication, recovery, and post-incident review.

17.6.6 Software and Updates

- Only approved software is allowed on Authority systems. Unauthorised software will be removed.
- Software updates and patches must be applied as soon as possible after release to minimise vulnerabilities.

17.7 Restrictions Imposed on Staff

17.7.1 Personal Device Use

- Personal devices, including smartphones, tablets, and laptops, are not permitted to access the local government network unless they are authorised and meet the security standards established by the ICT department.

17.7.2 USB Devices

- The use of USB storage devices is prohibited unless explicitly authorised. Any authorised device must be scanned for malware before use and where possible, encrypted.

17.7.3 Social Media Use

- Employees must refrain from posting sensitive government-related information on social media. They are not allowed to access social media accounts on government devices unless necessary for work purposes and pre-approved.

17.7.4 Remote Working

- Remote access to the local government network is only permitted via secure VPN, and only from Authority machines or using applications published with Microsoft Global Secure Access

17.8 Training and Awareness

- All employees must attend mandatory cybersecurity awareness training annually.
- Phishing simulations and other security drills will be conducted regularly to maintain high levels of vigilance.

17.9 Monitoring and Compliance

- The ICT department will monitor network traffic, emails, and system logs to detect and prevent unauthorised activities.
- Any breaches of this policy may result in disciplinary action, including termination of employment or legal action where necessary.

17.10 Policy Review

This policy will be reviewed and updated annually, or more frequently if required by changes in legislation or cybersecurity threats.

The cybersecurity policy should be **reviewed annually** to ensure it remains up to date with evolving cybersecurity threats, technological changes, and any updates to relevant laws and regulations.

Additionally, it should be **reviewed more frequently** if there are significant changes in the local government authority's ICT infrastructure, new threats or vulnerabilities are identified, or if there are updates in legal or regulatory requirements (such as amendments to GDPR or other data protection laws).

This ensures that the policy remains effective and aligned with current best practices in cybersecurity.