LDNPA – End User ICT Policies and information

This Policy applies to all LDNPA Staff and Members and any other personnel using LDNPA ICT systems and equipment.

Definitions

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

1. Your User Account
2. Hardware – PCs and Phones
3. Software
4. Email and Chat
5. Security
6. Managing your Data
7. Internet Use
8. Legislation

Version 1.0 – 2/9/2025 (This is a new standalone policy)

Review by 2/9/2028

Your User Account

Overview

Your user account identifies you on the Authority ICT systems.

- Keep your logon details secure
- Do not allow others to use your account
- Your account will lock for two hours if the password is entered incorrectly three times
- Your password needs to be at least 10 characters long, include a capital letter and a non-alphanumeric character (number, symbol)
- Your password expires every 6 months and will need to be changed
- If you believe your account has been compromised, change your password **twice**
- Report any concerns involving network security to the ICT Service

Hardware PCs and Phones

The equipment you receive will depend on your role and may include some of the following

- Windows Laptop
- Windows Tablet
- Android smart phone

ICT will monitor device usage and will reclaim under-used devices

You may not connect your personal or non-authority managed PC/Mac/Phone or other device directly to the Authority network or over VPN – an exception may be granted in special circumstances, for example Cumbria Woodland if there is no alternative solution and subject to ensuring such a device runs supported software, anti-virus and is fully patched.

Home/Remote Working

You can use your Authority laptop form home or other locations outside LDNPA Offices. To access internal systems such as Finance, HR and other in-house software, a client VPN is provided.

You must

- Ensure that you keep these up to date, for example, install updates promptly.
- Protect items from theft, do not leave unattended in public areas or in vehicles overnight
- Conduct a workstation risk assessment
- Keep items in good clean order, do not attach stickers etc to laptops etc.
- Contact the ICT service if you need to work outside the UK

You must not

- Install any software without consulting the ICT Service
- Allow anyone else to use your devices including family

You may

- Use your own PC or Mac to access Outlook and Teams at https://office.com (Web only)
- Use your own phone (iPhone or Android) to access Outlook and Teams
- Connect your laptop to public or home WiFi to access Authority systems

Refer also to the Computer Misuse Act 1990

Software

Your PC/Laptop will include Microsoft Office (Word, Excel, Powerpoint, Teams and Onedrive), 3cx phone system (for external calls) and windows defender antivirus

To protect your data, ensure OneDrive is running on your device and that work is saved into one of these locations:

- PC Desktop
- Documents Folder
- Pictures Folder
- Teams

Additional software **must** be sourced through ICT and may include:

- PDF Editor
- Visio
- MS Project
- Google Earth

All software requires licencing and additional cost will be incurred. **Do not** install any software from any source, including the Microsoft App store without permission from ICT Service, this includes Google Chrome.

Users are not granted Administration rights to PCs, this prevents the ability to install software in most cases.

Email and Chat

The Authority provides email services business purposes enabling you to communicate effectively and efficiently both internally and externally. All messages which are sent carry the identity of the Authority.

Email is provided for business purposes and messages may be searched for business reasons – such as to fulfil FOI requests

Incoming email is scanned for malware, spam/phishing content and profanity.

Links in emails are checked by the system but please be wary of mail which appears to be suspicious – we subscribe to a service which sends test phishing emails and direct you to training should you open a test link.

Teams Chat

- Teams Chats should be used for informal discussion around projects, operational activities, meeting arrangements etc. Co-ordinating with colleagues.
- Teams Chat should not be used for organising personal, out-of-work events; please continue to use your personal channels to do so
- Communication where retention of an audit trail is necessary- such as communications leading to a decision where a record must be kept email is still preferred for this use

Personal data must not be shared through chat systems

Links to shared locations should always be used in preference to attaching documents or other media to emails. Emails should be treated as non-secure.

Security

Even with the best security systems in place, there are still risks which you need to be aware of. Remaining alert to these risks can avoid problems.

Sign on to Authority systems is logged, this log includes date time and approximate location of sign-on.

Logs will be reviewed to detect suspicious sign-ins, usually from high risk countries.

- Sign-in from outside the UK is restricted by default – if travelling abroad for work, please notify the ICT service and your account will be de-restricted.
- Beware of email phishing attempts, these are becoming more and more sophisticated if in doubt, confirm by telephone using a known number
- The Authority subscribes to a Phishing training service which has been successful in helping staff spot phishing attempts, the service will send test emails periodically and offer training to those who need it.
- Review quarantined mail from Vipre
- Lock your PC when you are away from it
- Beware of others overlooking what you are doing if working on sensitive documents
- If you believe your account has been compromised change your password **twice** and contact the ICT service

- USB drives and other external storage media are blocked for write but may be used to read data from, however, cloud sharing is the best way to send and receive files
- Clean desk policy – do not leave documents on desks overnight, take laptops home or secure in a locker
- ICT systems will monitor logons for suspicious activity and to ensure PCs remain fully compliant
- We use Two Factor authentication for MS365 and VPN access and this must be configured during your induction
- You are responsible for keeping up to date on any security training requested to be completed by the ICT or People Team.

Managing your data

Ensure files are saved to Teams or OneDrive and that OneDrive is running without errors.

OneDrive will synchronise your desktop, documents and pictures folder to the cloud and across multiple devices.

Be aware of the recovery bin locations and version history, these tools will allow you to recover your own files if deleted or changed accidently

Use the sharing options in Teams and OneDrive to send and receive data between Authority members and external partners

Users leaving the Authority will have their Email and OneDrive assigned to their line manager for 30 days before final deletion, the line manager or delegate **must** ensure that any essential data is relocated before deletion.

Personal documents or other media should not be saved on any work devices or cloud storage facilities.

Internet Use

Internet is provided for business purposes, you can use it outside working hours (lunchtime etc) for personal use such as

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

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

Legislation

Users must comply with the following legislation.

- 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.
- Computer Misuse 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
- 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.