Wheelchair Alliance

Community Interest Company

'Strengthening your voice'

Information Communication Technology and Security Policy

Issue date: **13th February 2023 (unanimous ratification at Board meeting)**

Review date: **12th February 2024 or following legislative change**

Approved by: **Nick Goldup (Chair and director)**

Jon Sawford (Company Secretary, Safeguarding lead & director)

Ray Hodgkinson (Honorary Treasurer and director)

Table of contents

1. The Policy

This policy is not part of the employees' contractual term and conditions and as such changes may be made without consultation.

All those who have been granted access to use the Information and Communication Technology (ICT) Systems & Services provided by the Wheelchair Alliance are subject to this policy. It applies to use on any device that is owned by the Wheelchair Alliance or that is connected to any of the Alliance's networks or systems, no matter whether used while working from home or remotely anywhere in the world.

2. Purpose

This policy:

- Protects the Alliance's ICT Systems & Services from security risks;
- Ensures users are clear about what they can and cannot do;
- Helps the Alliance satisfy its legal obligations.

3. Definitions

A 'user' is defined as a member of staff, contractor or volunteer who has been granted access to use the ICT Systems & Services provided by the Alliance.

'ICT Systems & Services' are defined as the hardware, software, applications and digital services provided by the Alliance. This includes any software delivered as a service and Cloud services, including websites, supplied by third parties on behalf of the Alliance.

4. Principles

The Alliance recognises that ICT is an integral part of the way we work and encourages the active use of ICT Systems & Services to further our strategic aims and objectives.

ICT Systems & Services are provided primarily for business use, although occasional personal use is permitted as per section 11. Any ICT equipment provided, along with the data stored on ICT Systems & Services, remains the property of the Alliance.

The Alliance reserves the right to:

- Monitor and log use and access to equipment and ICT Systems & Services provided, including internet usage;
- Access, review, copy or delete any files, data, documents, messages or systems;
- Disclose the above to the police or other regulatory bodies, if requested;
- Remove unauthorised software installed on Alliance devices;
- Manage ICT Systems & Services on personal devices;

- Restrict or withdraw access to ICT Systems & Services.

Failure to comply with the policy can result in restrictions being placed on access to ICT Systems & Services and/or disciplinary action being taken.

5. Responsibilities

All **users** are responsible for:

- Ensuring they are aware of and comply with this policy and subsequent updates;
- Applying operating system updates when prompted;
- Complying with current legislation, including copyright laws;
- Adhering to software licensing terms and service terms of use and **must not** download software that has not been authorised by the Directors;
- Being vigilant to safeguard and protect ICT Systems & Services.

Users must not:

- Use ICT Systems and Services for any illegal or criminal activities or activities that could bring the Alliance into disrepute;
- View, download, create or distribute digital content that is:
  - Discriminatory or of a harassing nature;
  - Pornographic, obscene, sexist, racist, offensive, or illegal;
  - Derogatory or defamatory to any individual or organisation;
  - Contrary to the Alliance's policies or interests.

6. Hardware devices

Users must take reasonable care of ICT equipment provided by the Alliance. Portable devices, including laptops, must not be left unattended in public places or left on display in a vehicle, and where possible devices should be locked away or moved out of sight overnight.

Users must notify the Directors immediately if a device is misplaced, lost, stolen or damaged.

Any hardware provided by the Alliance which is no longer required or has reached the end of useful life must be returned as soon as possible for secure disposal.

7. Security Access and Control

Only authorised users are permitted to use ICT Systems & Services provided by the Alliance. Access to systems is controlled by passwords and, where possible, a second method of authentication. Any passwords must be kept private and not shared, displayed or communicated to others, including third parties and other family

members, and you must never use your primary Alliance password for other online accounts or services.

Strong passwords with a combination of uppercase, lowercase, numbers and symbols should be used and common usage words such as derivatives of 'password', names of family, friends, pets, co-workers, fantasy characters, birthdays or other personal information must be avoided.

Passwords should only be saved on devices provided by the Alliance. You should never save passwords for Alliance ICT Systems & Services on public devices.

To prevent unauthorised access, devices and monitors should be shut down and powered off when not in use for extended periods, and users should log off or lock their device when leaving it unattended for shorter periods. Mobiles and tablets must be protected with a password, PIN or fingerprint ID.

Users must not attempt to read or 'hack' into other systems or attempt to break into others' login accounts or passwords, or attempt to breach network security measures.

8. Data Storage

Data should primarily be stored on ICT Systems & Services; SharePoint or local network drives. This ensures data is readily available to those that need access, whilst safeguarding confidential or sensitive data. It also ensures data is included in regular backups and business continuity processes, as the recovery of data stored elsewhere, such as that stored locally on a mobile device, cannot be guaranteed.

Files and documents can be shared directly from SharePoint.

Users need to be mindful of personal, sensitive and special category data, as defined in data protection legislation, when storing and sharing data. If sharing personal, sensitive or special category data, users must be able to justify the purpose for needing to share the data, and the data must be encrypted if shared by email or systems other than SharePoint.

Non-sensitive data can be stored temporarily on removable media, such as USB storage, SD cards etc. providing any updated data is transferred back to Alliance ICT Systems & Services.

9. Emails and malware protection

Users must be vigilant with incoming emails and be wary of content that looks suspicious. Avoid opening suspicious emails and never click on any links or attachments within these. Notify the coordinator immediately if you suspect you've been the victim of an email attack, suspect you have malware on your device, or are not sure of the risk and need further guidance.

While in transit, the confidentiality of an email cannot be guaranteed. Where personal or sensitive data is sent outside of the Alliance via email, this must be encrypted or sent as password protected attachment and where possible the password should be sent via an alternative media, such as a text message. Passwords should not be sent in the same email as the attachment.

Where possible large files should be shared via SharePoint rather than sent as email attachments.

10. Personal Use

ICT Systems & Services are provided primarily for business use, but occasional personal use is permitted providing use is not abused and does not have a detrimental impact on Alliance business or network performance, and use is in accordance with the rest of this policy.

Exceptions to this are the download and/or the storage of personal photo or music libraries, games software, and unauthorised software.

Policy Review

The Company Secretary will review this policy on an annual basis in conjunction with the directors, and will make any changes necessary

All Board members are required to familiarise themselves with this policy upon their appointment to the Board.