

Smartwatch Policy – Access Control

General System Use

All users are granted the minimum level of system access to be able to do their job. You may not access or attempt to access systems, areas, information or assets to which you have not been specifically been granted authorisation to do so. Information assets and systems are checked for access levels on a regular basis.

Technical access controls are built into information systems by Smartwatch system suppliers. To ensure confidential information is protected, this functionality must be supported by operational and managerial controls put in place by Smartwatch.

The Access Control Procedure sets out how Smartwatch will allocate, manage, remove and monitor access rights to information systems so that only authorised personnel have access to use and share information held within those systems; and that access rights are used appropriately by the staff team. This policy aligns with the UK Data (Use and Access) Act 2025 and UK GDPR (as amended).

Failure to comply with the Access Control Procedure may be considered gross misconduct and so may lead to disciplinary action being taken against you. This policy aligns with the UK Data (Use and Access) Act 2025 and UK GDPR (as amended).

Responsibility for user access management

Smartwatch as assigned responsibility for managing user access rights to the system to the Company Director, who has administrator rights allowing access to sensitive areas (for example, HR, Accounts, Customer Information). The unnecessary allocation and use of administrator rights is often found to be a major contributing factor to the vulnerability of systems that have been breached, therefore allocation of administrator rights to other staff can only be authorised by the director Martin Hey.

Each user is identified by a unique user ID when granted system access. This ensures that users can be linked to and made responsible for their actions. During their induction to the system each user is given a copy of guidelines for staff on use of the system and their user login details, and is required to sign to indicate that they understand the conditions of access. A record is kept of all users given access to the system. Users are given the minimum access levels to do their job, additional access to other areas and applications should be requested via the Director of Operations

Change of user requirements

Changes to requirements will normally relate to an alteration to the level of access used or suspension of an account, e.g. if the user is on long-term leave or a temp staff member who

returns to Smartwatch from time to time. Requests are made to the Head of IT and an (email) record is kept of all changes.

Password management

The below is the outline of Smartwatch password procedure

All users should follow this guidance for choosing passwords to any systems.

- Use at least 8 alphanumeric characters, a mixture of upper and lower case and ideally add some special characters such as an underscore (_), a hyphen (-), a dollar sign (\$), a pound sign (£), a question mark (?), a forward slash (/), a hash sign (#) or a star (*) to further increase security;
- Choose a password that cannot be guessed and avoid using the names of children, partners, pets, your car registration number or football team etc;
- Systems often force a password change. Where this is not don't users should change their passwords at least every 3 months. Change your password regularly or immediately if you suspect someone may have guessed it;
- Never share your passwords with anyone, not even your closest colleague. If you suspect someone may know it, change it immediately.
- Do not write down your password, do not store in any filing systems (digital or otherwise)

Forgotten password

Where a user has forgotten his/her password, a replacement should be requested from the Head of IT, who issues a temporary, single use, password which requires the user to reset their password to one they are more likely to remember. In the event that the Head of IT is not available the IT suppliers are able to fulfil this requirement.

New Users and Removal of users

New users should only be created by the Head of IT or an authorised member of staff. All new staff members should be recorded on the HR induction checklist including systems they have been granted access to.

As soon as an individual leaves Smartwatch, all his/her system logons are revoked. As part of the employee termination process line managers inform The Head of IT of all leavers and their date of leaving. This also applies to third parties who have access.

Review of access rights

The Head of IT reviews all access rights on a regular basis, but in any event at least once a year. The review is designed to positively confirm all system users. Any lapsed or unwanted logons, which are identified, are disabled immediately and deleted unless positively reconfirmed. Monitoring compliance with access rights

The management of access rights is subject to regular compliance checks to ensure that this procedure is being followed and that staff are complying with their duty to use their access rights in an appropriate manner. Areas considered in the compliance check include whether:

- Only staff regularly working are registered as active users on the system;
- Allocation of administrator rights is restricted;
- Access rights are regularly reviewed;
- There is any evidence of staff sharing their access rights;
- Staff are appropriately logging out of the system.

Remote access

You may access Smartwatch information or systems from outside the office if you have been specially granted access to do so by the Head of IT. Please see mobile device and mobile working policy for more details.

Administrator and Privileged Access

Administrator accounts are restricted only to users who require them to do carry out their job role. You may not attempt to override, circumvent or access an area to which you have not been specifically granted access.

Privileged Applications

Applications that can over right permissions are referred to as "Privileged application". The business use of these applications is permitted to certain users only and recorded in the asset management system.

Signed:

Position: Managing Director



Name: Neil Jones

Date: 31/07/2025

Logging and Monitoring Access

Smartwatch implements logging and monitoring mechanisms to ensure that access to systems containing personal data is auditable and secure. All access to sensitive systems is logged,

including user ID, timestamp, and actions performed. These logs are reviewed periodically by the Head of IT to detect unauthorized access or anomalies. Logs are retained in accordance with the company's data retention policy and are protected against tampering or unauthorized access.