

Smartwatch has identified and mandate information security controls to specifically address supplier access to the organization's information this policy.

Supplier Policy

Smartwatch requires the security of its information to be maintained in order to ensure that Smartwatch is able to rely on its information for its business needs and meets its statutory, regulatory and legislative policy obligations. Supplier fall into 3 risk categories

- Low
 - Supplier has access to basic Smartwatch data (such as staff names, email addresses) but cannot access any other information
- Medium
 - Supplier has access to 1 or more systems that may contain confidential, commercial or customer sensitive material.
- High
 - Supplier has full access to all Smartwatch systems

Legislative, Regulatory and Contractual Requirements

Any organisation accessing, processing, communicating or managing Smartwatch's information must do so such that Smartwatch's legal, policy and regulatory obligations are met. Any processing of personal data outside the United Kingdom may only take place with the express permission of Smartwatch's director and prior to the commencement of any such processing. Arrangements for data processing will form part of a contract between Smartwatch and data processors.

Access to Smartwatch Information, Information Assets and Information Systems

Any organisation accessing Smartwatch information, processing information from Smartwatch and/or work in a Smartwatch building have a signed agreement detailing the rules on processing and the security agreements within a contract. If access is required to information at higher levels of security classification, additional national security vetting checks may be required.

Access to information assets and systems will be the minimum necessary to achieve business purposes. When the need to access Smartwatch information, assets and systems ends, all Smartwatch equipment (e.g. laptops, security passes, etc) must be returned to Smartwatch prior to the termination of a contract.

Smartwatch may monitor the use of its information, information assets and information systems for lawful business purposes.

Supplier personnel may only enter Smartwatch premises with an appropriate security pass issued by Smartwatch and may only enter areas of Smartwatch premises commensurate with their function and, where appropriate (for example, in security areas), escorted by Smartwatch staff.

Information Security Management System Controls

Where a supplier is contracted to manage Smartwatch information, information assets or information systems, the supplier must ensure that an information security management system employed to secure Smartwatch information. High risk suppliers must have systems in place certified to ISO/IEC 27001 (by a UKAS approved certification body). Evidence must be provided to Smartwatch of compliance with the standard, either through formal certification or otherwise to Smartwatch's satisfaction before any Smartwatch information, information assets or information systems are accessed by the supplier. Low or medium risk suppliers that are not ISO27001 certified the supplier must sign a "non disclosure agreement" (NDA) or have a contract adequately reflecting security obligations of the supplier.

Suppliers must agree to permit and facilitate audits of all aspects of their information security management system by Smartwatch and to address any findings of such audits in order to preserve the security of information to Smartwatch's standards and requirements.

The transmission of information between Smartwatch and a supplier must be encrypted to a level commensurate with the security classification of the information and to Smartwatch standards.

Live Smartwatch data and information may not be used for test purposes. Data and information to be used for test purposes must be sanitised, scrambled or otherwise rendered in such a way that no live Smartwatch data or information can be reconstructed from that used for test purposes.

Smartwatch information may not be copied by any supplier other than as far as is necessary for providing an agreed service to Smartwatch.

Suppliers must have a security incident reporting process in place to a standard and design acceptable to Smartwatch to ensure that any incidents involving Smartwatch information are immediately reported to Smartwatch. Suppliers must agree to undertake any remedial action required by Smartwatch and ensure that this is implemented in an auditable way.

A supplier holding Smartwatch data on Smartwatch's behalf must have in place processes to ensure that critical Smartwatch information held by them can be promptly and efficiently recovered following an emergency. Additional NDA (non disclosure agreement) may be requested by Smartwatch.

On Boarding new suppliers

The director must approve suppliers that have access to information systems. These should be entered onto the supplier spreadsheet with links to relevant contracts and NDA evidence.

Monitoring Suppliers

Suppliers are checked on a regular basis and recorded on the supplier management database / spreadsheet.

Signed:

Position: Managing Director



Name: Neil Jones

Date: 31/07/2025