

Acceptable Use Policy Summary

Overview

Stannp maintains strict acceptable use policies to protect our customers, employees, and the company from illegal or damaging actions. Effective security is a team effort requiring participation from everyone who interacts with our information and systems.

Access Control and Security

Access to Stannp systems is controlled through unique User IDs and passwords assigned to individual employees. All users are accountable for their actions and must maintain the confidentiality of their credentials. Unauthorised access, system modifications, and data transfers are strictly prohibited.

Data Protection Standards

All customer data processed by Stannp is classified as confidential and handled with the highest level of security. Employees must not store customer data on unauthorised equipment or transfer data outside the company. Unprotected confidential information must never be sent externally.

Internet and Email Use

Our internet and email systems are primarily for business use. Employees are prohibited from accessing, downloading, or sharing offensive, illegal, or copyrighted material. Official commitments on behalf of Stannp require proper authorisation.

Mobile Devices and Remote Work

Equipment taken off-site must be protected at all times. All mobile devices are secured with passwords or PINs and encryption where available.

Removable Storage Devices

Removable storage devices are strictly prohibited to protect data security. In exceptional circumstances where they must be used, only encrypted, company-authorised devices are permitted with approval from senior management.

Security Software and Approved Software

All company devices have automated antivirus software that must not be disabled or removed. Employees must use only software authorised by Stannp that is legally licensed, compliant with UK GDPR and Data Protection Act 2018, and regularly updated with security patches.

Monitoring and Compliance

System logging and monitoring occur to ensure security and effective operation, carried out in accordance with UK Data Protection Act 2018 and relevant UK legislation. All breaches of security policy are investigated and may result in disciplinary action.

Document Name:	TC-11	Version No:	2	Date:	17 th March 2025	Review Date:	17 th March 2026
----------------	-------	-------------	---	-------	-----------------------------	--------------	-----------------------------



Stannp.com

The Direct Mail Platform

Commitment to Customer Data Protection

These policies ensure that customer data handled by Stannp is protected through comprehensive technical and organisational measures, maintaining the confidentiality, integrity, and availability of all information processed on our systems.

Document Name:	TC-11	Version No:	2	Date:	17 th March 2025	Review Date:	17 th March 2026
----------------	-------	-------------	---	-------	-----------------------------	--------------	-----------------------------

www.stannp.com



Stannp.com



Stannp

Unit 12, Taw Trade Park
Braunton Road, Barnstaple, EX31 1JZ



01271 320 863



www.stannp.com

Stannp Ltd

Company Reg: 09086822

ICO Data Protection Reference: ZA134992