Acceptable Use Policy also see Information Classification

Objective and Scope

Acceptable use of information and other assets are the rules and standards established to ensure authorised use of the company's information and other associated assets, including computers, networks and systems, email, files and storage media.

The Acceptable Use Policy is key to mitigating security risks.

Roles, Responsibilities and Authorities

The Operations Director takes ownership of creating and assigning acceptable use standards.

Individuals shall be responsible for managing and following the acceptable access and use standards and the security of the information they handle ass a result of this access.

Legal and Regulatory

Title	Reference
Data Protection Act 2018	https://www.legislation.gov.uk/ukpga/2018/12/contents
General Data Protection Regulation (GDPR)	https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
The Telecommunications (Lawful Business practice)(Interception of Communications) Regulations 2000	www.hmso.gov.uk/si/si2000/20002699.htm
Computer Misuse Act1990	www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm
The Privacy and Electronic Communications (EC Directive) Regulations 2003	www.hmso.gov.uk/si/si2003/20032426.htm
The Freedom of Information Act 2000	https://www.legislation.gov.uk/ukpga/2018/12/contents
Online Safety Act 2023	https://www.legislation.gov.uk/ukpga/2023/50/contents/enacted
National Assistance Act 1948	https://www.legislation.gov.uk/ukpga/Geo6/11-12/29/enacted
Criminal Law Act 1967	https://www.legislation.gov.uk/ukpga/1967/58/introduction
The Copyright, Designs and Patents Act 1988	https://copyrightservice.co.uk/
Market Research Society Code of Conduct	https://www.mrs.org.uk/pdf/MRS-Code-of-Conduct-2019.pdf
Market Research Society Fair Data Principles	https://www.fairdata.org.uk/10-principles/

ISO 27001/2 REFERENCES	ISO 27001: 2022 Clause ID	ISO 27002: 2022 Control ID
Acceptable Use		5.10
Classification of Information		5.12

Acceptable Use Policy also see Information Classification

Related Information

- Information Classification Policy
- Physical (Equipment) Asset Management Policy (including maintenance and acceptable use of physical assets)

Policy - Network, Internet and Email Standards

Acceptable Use of Prevision Research IT Systems

- Access and use of IT systems and facilities must be for legitimate work purposes.
- Access and use of IT systems for personal reasonable and legal use is acceptable as long as it does not adversely affect business needs. This use is considered a privilege and not a right. It can be withdrawn at any time.

Unacceptable Use of Prevision Research IT Systems

- Creating, using, saving or distributing material that might reasonably be considered offensive, obscene or indecent by an ordinary member of the public e.g. pornographic or racist.
- Piracy such as plagiarising, copying or distributing information in contravention of copyright and similar legal obligations.
- Sharing or disclosing personal user identities, passwords, or other secure ID with others
- Connecting Prevision Research devices to other networks without the permission of the DoT.
- Monitoring, intercepting or otherwise accessing network traffic, emails, files etc. intended for another person.

Acceptable Use of Prevision Research Internet Access

- Accessing information from the Internet and using general Internet services (such as email) for legitimate work purposes.
- Accessing and using the Internet for personal purposes, provided such use is incidental and reasonable, does not conflict with other network or Internet use, and does not constitute unacceptable use.

Unacceptable Use of Prevision Research Internet Access

- Up/downloading or distributing illegal material or visiting websites that might be considered offensive, obscene or indecent by an ordinary member of the public (e.g. pornographic or racist)

Acceptable Use Policy also see Information Classification

- Making additional Internet connections, even temporarily, without authorisation or without applying appropriate IT security controls.
- Storing corporate or personal information on Internet-based backup or file server sites without strong encryption

Acceptable Use of Prevision Research Emails

- Prevision Research staff show be coached in the detection and reporting of suspicious email. This may include the regular and frequent sending of simulated phishing emails and targeted training to staff.
- Emails must be classified using information classification standards based on confidentiality, integrity and availability (CIA) when considering precautions when sending/receiving emails.
- User email accounts must not share a password.

Compliance

Repeated non-compliance with this Standard may result in disciplinary action, including legal action.

Suspected unauthorised disclosure or modification

Report any lost, damaged property, unauthorised access/use or suspected malware activity immediately to management. Provide details regarding likely impact on data security and effects on company or client information.

Policy review

This policy shall be reviewed by the policy owner annually or immediately after a process change or a policy breach is known to have occurred.

Periodic reviews shall take into account feedback from management reviews, regulatory changes and audits. Changes to the policy must be approved by a senior executive and then communicated to all previous persons or organisations with access to the policy. Refer to below for the most recent review.

History table

Date	Rev No	Changes	Reviewed By	Approved By	Training Y/N