Strength & Conditioning Education

Policy

IT Asset Management

1 Introduction

SCE has a responsibility to manage both its IT *and* Information Assets, which stems from a number of requirements:

- Legal / Regulatory
  - General Data Protection Regulation (personal data / information asset management / data breach management)
  - Data Protection Act
  - Computer Misuse Act
- Contractual
  - Security requirements (e.g. encrypted hard drives, OS and software update)
  - Equipment lifecycle management (commissioning and disposal)
- Licensing
  - Appropriate products on appropriate machines, as per corporate or individual licensing stipulations

1.1 Purpose

This policy aims to ensure that all SCE-issued IT devices report appropriate information to centralised information stores, in order for SCE to provide better assurance it is meeting its legal, regulatory, contractual and licensing requirements.

Under the General Data Protection Regulation, individual contracts with data suppliers, and SCE's duty of care to its community, it is important to ensure that information on IT assets is protected, maintaining the principles of 'least privilege' and 'need to know'.

1.2 Scope

All IT devices purchased, run, managed or issued by SCE.

1.3 Out of Scope

Personally owned IT devices, or devices issued by other organisations. Users of such devices should, however, be aware of and abide by their obligations under all applicable laws, the SCE's *Information Security Policy*, subsidiary policies, any contracts and all licensing agreements when these devices are used to access, store or process data where SCE is either the data controller or the data processor.

Local printers and other 'dumb' devices onto which agents cannot be installed must be recorded via asset tags. All devices purchased will have such asset tags; it is the responsibility of other purchasers to ensure such items are appropriately recorded.

2 Policy

2.1 IT Device Asset Management

All IT devices purchased, run, managed or issued by SCE will be manually added to an asset management store.

Information asset management will be covered by a separate policy, in accordance with the requirements of the EU General Data Protection Regulation.

2.2 Software

Any software installed must be legitimately purchased and licensed for the use made of it. It is the responsibility of each user to ensure that any non-centrally-licensed software is legitimately purchased, deployed and used.

2.3 Asset redeployment

SCE-owned IT assets – hardware, software, licences, cloud services – that are no longer in use must be returned to SCE for redeployment.

2.4 Non-compliance

All SCE IT Devices, as specified above, must comply with this policy. Breach of this policy may result in any device being remotely wiped, blocked from SCE's network, blocked from using SCE-provided services and software and may be considered a disciplinary offence.

2.5 Incident Handling

If a member of SCE (staff or student) is aware of an information security incident that materially breaches this policy, then they must report it to the Data Protection Officer (DPO) at Info@strengthandconditioningeducation.com or telephone 0113 237 9667.

2.6 Review and Development

This policy, and any subsidiaries, shall be reviewed by the GDPR Readiness Team (GRT) and updated regularly to ensure that they remain appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.

Additional regulations may be created to cover specific areas.

GRT comprises representatives from all relevant parts of the organisation. It shall oversee the creation of information security and subsidiary policies.

The DPO will determine the appropriate levels of security measures applied to all new information systems

3 Responsibilities

GDPR Readiness Team

Provide the appropriate centralised IT asset management stores for the receipt of SCE IT Device information, as required by the legal, regulatory, contractual and licensing requirements outlined. Provision of client-based or clientless monitoring in order to extract such information.

Responsibility for reviewing and maintaining this policy.

Data Protection Officer

Responsibility for Information Asset Management policies.

IT Device users

Ensure their devices meet this policy. Report any breaches of this policy.