Information Technology Policy

Purpose of the policy

This policy sets out Sport Structures guidelines on digital data and electronic equipment usage.

Scope of the policy

This policy applies to all employees, including those who work part-time or on fixed-term contracts.

Role and responsibilities

At Sport Structures:

- line managers are responsible for ensuring their team complies with this policy
- employees are responsible for following this policy and for informing their line manager of any IT related issues
- the Director of Digital Technology is responsible for reviewing this policy once a year

Devices

Sport Structures will provide employees with all electronic devices required to do their job. This may include but is not limited to a:

- laptop
- mobile phone
- headphones and microphone (office only)
- second screen (office only)
- docking station (office only)

In addition, staff can request further IT equipment if required to support a specific learning need. These requests will be considered on a case-by-case basis to ensure appropriate support and accessibility.

If a member of staff wishes to use additional equipment in their home office, such as a second monitor, this should be requested through the Director of Digital technology. Any equipment purchased by the company will remain the property of the company and not the individual employee.

All devices/equipment are primarily for business use. Reasonable personal use on business devices is allowed. Excessive personal use on business devices may result in disciplinary action under the company's disciplinary procedure.

Examples of personal use of business devices that are unacceptable are:

- viewing inappropriate or pornographic material
- excessive use of the internet during work time on non-work-related websites
- watching television programmes or live streams
- playing games
- downloading
- online shopping
- searching for jobs online

This list is not exhaustive.

Sport Structures reserves the right to use monitoring software to check an employee's use of business devices. This will be used for legitimate purposes only and to ensure there is no abuse of trust.

Details of data kept and the reasons for this are available in Sport Structures' privacy policy. This can be found on the Sport Structures website and on the staff SharePoint site.

Employees are not permitted to use their personal devices for work purposes. Unless specifically agreed with managers to overcome potentially other technical issues with Sport Structures equipment. Personal devices can be used by employees during lunch and breaks.

Employees are responsible for the safekeeping of devices provided by Sport Structures.

Issues with devices

All devices issued to employees have been checked by the Director of Technology. They are sufficient and will enable the employee to perform their job to the required standard. All laptops have been installed with Sport Structures' chosen anti-virus and security software.

It is the responsibility of all employees to keep the software on their computer up to date. Employees are strongly recommended to fully close their computer at least once a week and when they are on leave to ensure updates are installed.

Employees should not try to resolve any issues themselves. This will be done by CloudClevr's IT technicians.

Where a problem cannot be resolved by CloudClevr's IT technicians, the employee will be encouraged to speak to the Director of Technology. It is likely that a replacement device would be issued.

Devices and equipment when working away from the office

When employees are working away from the office, they must take steps to ensure the safety of Sport Structures equipment and information. Employees must:

- work in a secure environment
- not use their personal devices for work, unless agreed in advance

- not allow others to access their work or work equipment
- lock screens on devices when away from them
- securely lock devices away when they are not being used
- not leave devices unattended or allow them to be outside of their possession
- change their home router password so it complies with this policy
- configure their router to block all unauthenticated connections by default
- disable the administrative interface for external user access (via the internet) on their home router

Sport Structures employees are not permitted to work in public places or use unsecured Wi-Fi networks or connections. Either of these can easily result in UK General Data Protection Regulation (GDPR) and security breaches.

If employees encounter any issues with their device or connection while working away from the office, they should contact CloudClevr straightaway

Training

At the start of their employment employees will be given basic IT training by a member of the Digital Technology Team. This will include:

- setting up accounts and passwords for login accounts
- how to use Sport Structures SharePoint
- how to use the Sport Structures Learner Management System
- advice on how to keep information safe and where to store it

Following initial training, if employees have any issues using IT equipment, accounts or the systems they should contact the Director for Digital Technology.

UK GDPR, cyber security and information security

Email, company IT systems and servers are often targeted by hackers. If the structures are compromised it can lead to confidentiality breaches, viruses and malware.

Sport Structures has responsibilities to protect data it stores.

Sport Structures has firewalls and anti-virus programs in place to help keep the business secure. Doing this ensures that Sport Structures complies with its obligations under UK GDPR. Employees are not permitted to obtain their own security or anti-virus software for their work devices.

To help protect the sensitive information dealt with by Sport Structures, employees should be vigilant and do the following:

Passwords

At Sport Structures employees should:

- select strong passwords using a mixture of letters, capital letters, numbers and symbols
- when selecting a password, avoid personal information such as birthdays, names, or common phrases
- store passwords in a safe place not accessible electronically
- not disclose passwords to anyone
- not reuse passwords

Emails

Employees should:

- be aware of email scams and phishing emails
- if in receipt of a suspicious email, forward the email to report@phishing.gov.uk do not forward to anybody else or reply. If you are not sure, contact CloudClevr support or the Director of Technology to be checked before opening
- not open attachments of suspicious emails

Our devices are password encrypted to make sure no one other than the device user (or Sport Structures' IT personnel) can use it.

Confidentiality

Information obtained for work purposes and during an employee's employment with Sport Structures must be treated confidentially and stored securely. This means the employee must:

- only use information obtained for work purposes
- store information obtained on the secure IT system
- not store information on their desktop
- not discuss information obtained with colleagues not relevant to the job
- not discuss information obtained with anyone outside of the business

Use of email

The points below are guidelines on the access and use of email:

- email is to be used for Sport Structures business needs and not for excessive personal use
- emails are not to be encrypted unless the content is sensitive or employees are instructed to do so by a Senior Manager
- Sport Structures email is not to be used for illegal or wrongful purposes
- employees are not to use Sport Structures email systems to infringe on copyright or intellectual property rights
- employees are not to use Sport Structures email systems to distribute defamatory, fraudulent or harassing messages

- emails relevant to the course of business at Sport Structures should be filed as per existing procedures for written correspondence
- email accounts are only to be used by the person it is assigned to
- employees are not to share their account names or password
- subscription to mailing lists, bulletin boards, chat groups and other information services is not permitted
- sending and receiving pornographic or other offensive material is prohibited
- sending any emails that maybe deemed as politically sensitive should not be sent.

Sport Structures reserves the right to use monitoring software to check use and content of emails. This will be used for legitimate purposes only. Users should be aware that even after an email has been deleted from the system, backup copies are still available.

Details of data kept and the reasons for this are available in Sport Structures's privacy policy.

Information storage and data backups

All Sport Structures' electronic information will be stored on centralised and secure cloud servers to allow regular backups to take place.

Employees are not to save any information anywhere other than on Sport Structures' secure networks and servers. This is to ensure any information lost can be recovered easily. This also safeguards information in the event of a lost device.

Employees are not permitted to save, download or transfer any information stored on these systems onto any other device. The only exception is to download onto another business device for work purposes.

Transferring data onto anything other than a work device or not for work purposes will be treated as a security and UK GDPR breach.

Downloading software

Sport Structures devices have all software employees require to perform their job. We however recognise there may be occasions employees require software not available on Sport Structures's systems. Employees are required to keep their software up to date and follow regular prompts set by our IT company to update software periodically.

If an employee requires access to software not already on Sport Structures's system, they should submit a request to the Director of Technology outlining the purpose and necessity of the software. The request will then be reviewed to assess compatibility, security, licensing, and cost implications before approval is granted.

The use of company software such as Microsoft 365 on personal devices is permitted, if necessary. Your device must comply with our security protocols, be password protected, have regular software updates and use multi-factor authentication.

Incident response

A breach or potential breach of security is classed as any incident which exposes sensitive personal data or confidential information to an unintended recipient. This definition covers a wide range of events and Sport Structures cannot list all eventualities.

When there is a breach or potential breach of security, the following protocol must be followed:

1. Try to recall the information immediately if possible.
2. If the information cannot be recalled report the incident to your Line Manager for immediate corrective action.
3. The Director of Digital Technology should also be contacted to advise an urgent response is required.
4. Report the incident to the appropriate line manager.
5. In the reports include a detailed description of the security breach.

Each incident will be assessed based on the potential detriment to the person/organisation affected. Assessment will consider the severity of the breach as well as the amount of data involved.

Breaches of this policy

Any breaches of this policy will be thoroughly investigated and could result in disciplinary action