

Information Technology Policy

Purpose of the policy

This policy applies to all employees, including those who work part-time or on fixed-term contracts. Its purpose is to ensure that information technology, digital systems and electronic equipment are used securely, responsibly and appropriately to support our operations, protect confidential information and personal data, and reduce the risk of cyber security incidents.

The policy establishes clear expectations for the use of company equipment, email, software, digital platforms and information systems, including when working remotely. It also explains the responsibilities of staff in maintaining information security and reporting IT issues or potential security incidents.

Scope of the policy

This policy applies to all employees, including those who work part-time or on fixed-term contracts. It also applies to associates, contractors and any other individuals who are authorised to access Sport Structures' IT equipment, systems, accounts or information. References to "staff" throughout this policy apply to all individuals within its scope.

This policy should also be considered in conjunction with the following (list not exhaustive):

- Data Protection Policy
- Privacy Policy
- Cultural Code for Staff and Workforce
- Disciplinary Policy

Role and responsibilities

At Sport Structures:

- The Chief Executive Officer and Head of Commercial is responsible for reviewing this policy once a year and ensuring it is included in any staff/associate induction process and is available to all staff and associates for reference

- Line Managers are responsible for ensuring that staff understand their responsibilities and know how to report IT problems or security concerns.
- Employees and associates are responsible for reading and following this policy

All staff are responsible for protecting the equipment, accounts and information they access, completing required IT and information security training, and reporting suspected security incidents promptly.

The Head of Commercial is responsible for overseeing the policy's implementation, coordinating with the external IT support provider where necessary, and ensuring that reported IT and security issues are appropriately escalated.

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
- second screen
- docking station

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 Head of Commercial. 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 procedures. 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 programmes / app without prior permission
- 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.

Any monitoring will be carried out proportionately, for legitimate business purposes and in accordance with applicable data protection requirements. Further information about monitoring, the information collected and how it is used is provided in the Privacy Policy.

Staff must not use personal devices for work purposes unless authorised by their manager to meet an agreed business need. Where authorised, personal devices must meet Sport Structures' security requirements and be used in accordance with this policy.

Staff may use Zoom on a personal mobile phone or other personal device for business calls where this has been approved and the Zoom account is provided by Sport Structures. Staff must use the Sport Structures Zoom account when making or receiving business calls, must not share personal contact details where this is not necessary, and must take reasonable steps to protect confidential information when using the service.

Employees are responsible for the safekeeping of devices provided by us. Company equipment must be returned promptly when requested or when employment or an associate arrangement ends.

Issues with devices

Sport Structures will provide equipment suitable for each employee's role. Employees should report any concerns about its performance, suitability or accessibility to the Head of Commercial so that these can be reviewed. All laptops have been installed with Sport Structures' chosen anti-virus and security software.

Employees must follow update prompts and instructions issued by Sport Structures or CloudClevr, including restarting devices when required. Updates must not be repeatedly postponed. Any failed updates or uncertainty about an update prompt should be reported to CloudClevr. 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 may carry out basic troubleshooting in line with approved guidance, such as restarting a device or checking connections. They must not change security settings, install unapproved software or attempt repairs. Unresolved faults and suspected security incidents must be reported to CloudClevr.

Where a problem cannot be resolved by CloudClevr's IT technicians, the employee will be encouraged to speak to the Head of Commercial. It is likely that a replacement device may be issued where appropriate.

Staff must not disable security settings, install unauthorised software or attempt to bypass IT controls. Any suspected malware, unusual device behaviour, loss of access or security warning should be reported promptly to the IT support provider and, where appropriate, the Head of Commercial.

Remote and flexible working

We operate a remote working model. All staff are responsible for ensuring that company equipment, systems and information remain secure when working from home or any other authorised location.

Employees must:

- Ensure that company devices are kept secure and protected from loss, theft or unauthorised access.
- Lock their devices whenever they are unattended and shut them down or secure them appropriately when not in use.
- Ensure that other household members or third parties cannot access company devices, accounts or confidential information.
- Take reasonable precautions to prevent confidential information being viewed or overheard by others.
- Use secure internet connections and ensure home Wi-Fi networks are protected by a strong password and appropriate security settings.
- Keep devices and software up to date and follow any security requirements set by Sport Structures or its IT support provider.
- Store work-related information only in approved company systems and locations

Staff should normally work from a secure private location. Where working from another location is necessary, they must ensure that the environment and internet connection are appropriate for the work being undertaken. Public or unsecured Wi-Fi networks must not be used to access company systems unless an approved secure connection, such as a company-approved VPN, is in place.

Confidential conversations and information must not be exposed to people who are not authorised to access them. Staff must not leave company devices unattended in public places or in vehicles where they may be vulnerable to theft.

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 our SharePoint
- how to use our 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 Head of Commercial. Staff must complete online safety training as required by Sport Structures and apply the guidance provided in their day-to-day work.

UK GDPR, cyber security and information security

Email, company IT systems and servers are often targeted by hackers. If these systems 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. These safeguards form part of Sport Structures' wider technical and organisational measures to protect personal data and support compliance with 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:

- Use a strong, unique password for each work account. Use a long passphrase, such as three random words, where the system allows.
- Avoid passwords based on personal information, common phrases or predictable patterns.
- Never reuse work passwords for personal accounts or across different work accounts.
- Never share passwords with anyone, including colleagues.
- Never record passwords in unsecured documents, emails or notes, or leave them where others could access them.
- Enable and use multi-factor authentication where required.

- Report any suspected password compromise to CloudClevr immediately and change the affected password promptly.

Staff must not share accounts or allow another person to use their login credentials. Multi-factor authentication must be enabled and used wherever required by Sport Structures. If a password may have been compromised, staff must change it promptly and report the concern to IT support.

Emails

Employees should:

- be aware of email scams and phishing emails
- Check suspicious emails carefully, including the sender, links and attachments
- Not open attachments or click links in suspicious emails

If you receive a suspicious email:

- Do not reply, click links or open attachments.
- Contact CloudClevr for advice. Do not forward the email to colleagues. If CloudClevr needs a copy, follow their instructions for providing it.
- Suspected phishing emails can also be forwarded to report@phishing.gov.uk. This does not replace reporting the concern internally.
- If you have already clicked a link, opened an attachment, shared information or approved an unexpected authentication request, contact CloudClevr and the Head of Commercial immediately. Report what happened, even if nothing appears to be wrong.
- If CloudClevr is unavailable, contact the Head of Commercial without delay.

Staff must never disclose passwords, payment details or sensitive information in response to an unexpected email or request without independently verifying its legitimacy. Company laptops are protected by password-controlled access and full-device encryption. Staff must not disable or bypass these protections.

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

Only share confidential information outside the business where this is authorised and necessary for work, using an approved method and following relevant data protection requirements.

Staff must take particular care when handling learner records, employee information, financial information, safeguarding information and other sensitive or confidential material. Information must only be accessed, shared and retained where there is a legitimate business purpose and appropriate authorisation.

Confidential information must not be sent to personal email accounts, uploaded to unapproved cloud storage or transferred to unauthorised devices.

Use of email

Email should be used primarily for Sport Structures' business needs and not for excessive personal use.

- Emails must not be used for illegal or wrongful purposes.
- Sport Structures email systems must not be used to infringe copyright or intellectual property rights.
- Staff must not distribute defamatory, fraudulent, harassing or offensive messages.
- Emails relevant to the course of business at Sport Structures should be filed in accordance with existing procedures for written correspondence.
- Email accounts must only be used by the person to whom they are assigned.
- Staff must not share account names or passwords.

Staff must not deliberately access, send, request or circulate pornographic or other offensive material. Unsolicited material should be reported where appropriate and handled in accordance with IT guidance. Legitimate handling of material for an authorised safeguarding or investigative purpose must follow the relevant procedure.

Staff must take care to check recipients and attachments before sending emails, particularly where personal, learner or confidential information is involved. Where sensitive information needs to be sent, the approved secure sharing or encryption process must be followed.

Work email must not be used for personal commercial activity, unauthorised political campaigning or other activity that could compromise Sport Structures' reputation or operations. Legitimate professional discussion of political or public policy matters is not prohibited solely because the subject is politically sensitive.

Sport Structures reserves the right to use monitoring software to check use and content of emails. This will be used for legitimate purposes only. Staff 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 our 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.

Work information must be saved in approved company systems and storage locations. Local copies, downloads and offline working are only permitted where authorised and protected in accordance with company guidance. Staff must not use personal email accounts, personal cloud storage or unapproved storage devices for work information. 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.

Information must not be transferred to personal storage devices, personal cloud accounts or other unapproved services. Any approved transfer must be necessary, appropriately secured and compliant with data protection requirements.

Staff must follow the organisation's retention and disposal requirements and must not retain personal or confidential information longer than necessary.

Downloading and installing 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 our 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 our system, they should submit a request to the Head of Commercial 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.

Use of company software on personal devices is subject to the approval and security requirements in the "Use of personal devices" section.. Your device must comply with our security protocols, be password protected, have regular software updates and use multi-factor authentication.

Staff must not install unapproved applications, browser extensions or other software, or connect unauthorised devices to company systems.

Use of personal devices

The use of company software, such as Microsoft 365, on personal devices is permitted only where necessary and specifically authorised.

The device must comply with Sport Structures' security protocols, be password protected, have regular software updates and use multi-factor authentication where required.

Staff must not download or store company information locally on personal devices unless explicitly authorised and necessary for the agreed purpose. Sport Structures may withdraw access where a device no longer meets security requirements.

Use of Artificial Intelligence

Staff must only use artificial intelligence (AI) tools and external digital services in accordance with Sport Structures' approved arrangements and any relevant organisational guidance.

Personal data, learner information, safeguarding information, confidential business information and commercially sensitive material must not be entered into public or unapproved AI tools or external services.

Staff remain responsible for checking the accuracy, appropriateness and confidentiality of information produced or processed using AI tools. AI-generated content must not be treated as authoritative without appropriate human review. Where a proposed tool involves processing personal data or confidential information, approval must be obtained from the Head of Commercial and, where appropriate, the relevant data protection lead before use.

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. Report the incident to your Line Manager for immediate corrective action.
3. The Head of Commercial 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.

The Head of Commercial and relevant senior personnel will ensure that incidents are escalated appropriately and that any required data protection assessment, corrective action and regulatory or individual notification are considered in accordance with applicable requirements.

Breaches of this policy

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

Where the policy is breached by an associate, contractor or other non-employee, Sport Structures may take appropriate action in accordance with the relevant agreement, which may include restricting access to systems or ending the arrangement.

Staff are encouraged to report concerns or mistakes promptly. Reporting an incident in good faith will help Sport Structures respond appropriately and reduce potential harm.