Cyber Security Policy

1. Introduction

This policy applies to all employees and volunteers of YMCA Brunel Group, and its subsidiary Bath YMCA Trading, as from 01 July 2021. It sets out the framework that covers the organisation's approach to cyber security and the necessary measures put in place to protect the organisation.

The risk of data theft, scams and security breaches can have a detrimental effect upon a company's infrastructure, systems and reputation. YMCA Brunel Group have introduced this policy to help to outline the security measures put in place to ensure that information remains secure and protected and that IT systems can function reliably and safely.

2. Expectations & Policy Compliance of the Organisation

As a team member, we expect you to:

- Behave honestly, responsibly and within the guidelines of this policy
- Ensure you have a good understanding of the IT equipment and software that you need to carry out your job role
- Undertake any necessary formal or informal training needed to use IT equipment securely
- Always maintain good confidentiality

As a manager, we expect you to:

- Have a good understanding of the IT equipment and software needed in your department and take a lead role in ensuring it is used appropriately and securely
- Ensure that access to IT equipment and software is arranged and ended appropriately for your team when starting, changing role or leaving
- Ensure you and your team(s) have a good understanding of the requirements of this policy – contacting the HR department regarding training as needed

If employees do not comply with the policy, we may review the allocation of equipment or access to systems which may impact the ability to perform a role. Persistent or deliberate non-compliance may result in disciplinary action.

3. IT Access & Infrastructure

Access to the organisation's IT systems is only given to team members who require this access to perform their job role.

New team members, or those whose job role changes so that access becomes necessary, have a named account organised for their use by the HR department. Accounts are created by the person(s) responsible for IT in the organisation, or the Chief Executive who holds overall responsibility.

Each named account is allocated a secure password. It is the responsibility of all team members to keep their login details and password totally confidential. These should not be shared with anyone under any circumstances

Access can be reset or terminated when needed by contacting the HR department.

Once a team member has access to the organisation's IT system they may also be issued with login details for specific software needed to perform their job role. This access is also password controlled and account details must be kept totally secure by the team member.

It is not permissible to create written records of account details and passwords under any circumstances. Team members are required to memorise their passwords. If a password to software is forgotten it can be reset by contacting the person responsible for the area of work or the person designated to lead on the software.

Team members are only permitted to access the software needed for their role using devices issued by the organisation.

Passwords must be reset on a regular basis to ensure good security. This is a requirement of the insurance cover of the organisation as well as an important measure for general cyber security. The organisation defines regular as a minimum of every three months.

Administrator permissions on devices is not given to any individual member of staff. The administrator login details are held by the Chief Executive and nominated IT responsible persons only. This is to protect against malicious software making changes on devices without the knowledge of the device user. Changes that require an administrator login will be assessed by the Chief Executive or nominated IT responsible person before the login can be used on the device.

YMCA Brunel Group uses Microsoft Office 365 with data is saved in the cloud. The organisation employs the services of a backup system to ensure that backups are made for all data saved using Office 365.

Each area of work uses software relevant to the nature of the work. This is to store and manage data as well as to provide financial information. All new software must be vetted by the senior manager, finance director and Chief Executive before being approved for us. It must meet data security requirements, operating requirements and be able to provide suitable financial data.

4. Devices

YMCA Brunel Group issues devices for the use of team members for them to perform their job roles as defined in the job description of each role.

Devices may include:

- Laptops
- Office computers
- Mobile phones
- Desk phones
- Tablets
- Other electronic devices

Line managers are responsible for liaising with HR to ensure that devices are appropriate for the role. HR will liaise with IT to ensure that requests for new devices are submitted, and the returns of equipment no longer needed are processed.

YMCA Brunel Group requires that all devices are password protected. Team members must ensure that protection is not removed from a device. Devices may not be shared or passed on without liaising with HR (apart from desk computers which may be used by any member of staff using their own login).

Devices belonging to YMCA Brunel Group should be used for approved purposes only.

Social media access on devices owned by YMCA Brunel Group should be for work purposes only. The use of personal social media on work devices is not permitted.

5. Email Security

Ensuring good security of email systems is a high priority for the organisation as emails can lead to data theft, scams, malicious software and other threats.

YMCA Brunel Group requires all employees to:

- Use email accounts securely and for approved purposes only
- Access email on approved WIFI and network connections only
- Maintain good security of passwords
- Verify the legitimacy of each email, including the email address and sender name
- Avoid opening suspicious emails, attachments and clicking on links
- Look for significant grammatical errors
- Avoid clickbait titles and links
- Check your spam folder carefully and only whitelist or approve emails that you have verified
- Raise queries with the person(s) responsible for IT directly but without forwarding potentially damaging emails

Transferring data through email should be done in line with the organisation's GDPR policy. Egress accounts are available to all staff on a limited basis to ensure that personal data can be sent using secure encryption. Frequent users of Egress can be issued with a business licence to ensure sufficient capacity.

Before sending emails containing personal data, even via Egress, it is vital that team members check the recipient details very carefully. For highly sensitive items team members are required to send a test email first to ensure that the email address will correctly reach the intended recipient.

Where a team member has concerns about how to ensure security is maintained and that GDPR requirements are compiled they should contact their line manager or another senior member of staff.

Requests for payments received by email should be scrutinised by the team member, budget holder and finance department in line with the contracts and procurement policy.

6. Security Breaches

If a team member suspects that a security breach has occurred, it is essential that this is reported to their line manager (or another senior manager) and investigated immediately.

If the breach could lead to a data breach this must be reported to the Information Commissioner's Office within 72 hours, in line with the GDPR policy, so speed is of the utmost importance.

Additionally, to minimise the impact of a cyber security breach it is vital that action is taken as quickly as possible.

Due to the nature of the breach the report should be made by phone initially, until the Chief Executive or nominated responsible IT person(s) have assessed the breach. Instructions will then be given to the team member.

If a team member deliberately or maliciously enables or perpetrates a security breach this will result in disciplinary action and may be reported to the police for criminal proceedings.

7. Training

All staff should receive suitable training to ensure that they understand the importance of cyber security and how to use the devices and systems safely that are necessary for the role they need to perform.

Training may be formal where required however for most staff this can be covered informally in the induction and by reading and understanding the policies of the organisation. It is the responsibility of line managers to identify training needs and arrange suitable formal or informal training as needed, through liaising with the HR department.

8. Accountability

The team member is accountable for:

- Ensuring a good understanding of this policy and how to safely use the devices and software necessary to perform their role
- Keeping passwords and login information secure
- Not sharing login information with anyone
- Ensuring a good understanding of data protection requirements and the policy of the organisation
- Using access to the IT system and software responsibly and maintaining strict confidentiality
- Reporting concerns about suspicious emails or unusual activity/appearance of devices to a line manager or other senior manager immediately
- Attending and completing any informal or formal training needed

The manager is accountable for:

- Ensuring all team members receive suitable formal or informal training in their induction to be able to safely use the devices and software required for their role
- Identifying training needs and liaising with HR to ensure all staff are sufficiently trained
- Requesting access set up, changes and termination for all staff as needed

- Handling initial queries or concerns about potential breaches and ensuring that suitable referral is made to a senior manager or the Chief Executive
- Ensuring good cyber security and data protection practices are fostered and maintained in their department

The Chief Executive is accountable for:

- Overall IT system security and ensuring appropriate technical support is in place for the organisation
- Approval of any new software or system changes
- Oversight of access management
- IT equipment upgrade assessment and purchase
- Dealing with cyber security breaches

9. Queries

If there are any queries relating to this policy, please contact the senior manager of your area of work or the IT nominated responsible person for the organisation.

Signed on behalf of YMCA Brunel Group (original signed copy held at registered office)	 Mike Fairbeard
Role of Signatory	Chief Executive
Date of Review of Policy	January 2027
Approved by trustees	31st January 2026