YMCA DERBYSHIRE

Information Technology, Data Security and Data Retention Policy

Department: Core Services

Approval Route: Board

Frequency of Revision: Biennial

Lead Policy: **Data Protection Policy**

Linked Policies and Procedures:
CCTV Policy
Disciplinary Policy

Version	Date Approved	Reason for Update
1	**22 July 2024**	Combines previous policies and procedures: • Computer Policy • Information Security Policy • IT and Data Security Procedure • Data Retention Procedure.

Table Of Contents

Appendices
Appendix 1 - Email Etiquette and Content
Appendix 2 - Retention Schedule for YMCA Derbyshire Services

1. Policy Statement and Scope

1.1 The information technology systems and equipment ("IT") of YMCA Derbyshire (the "Association") are highly valued assets intended to promote effective communication and working practices that are critical to the success of our business. This policy deals with the use and misuse of IT and aims to protect these assets, to reduce the risk of security incidents and to demonstrate to employees and service users that we collect, handle store and dispose of their information securely. It outlines the standards we require users of these systems to observe, the circumstances in which we will monitor use of these systems and the action we will take in respect of breaches of these standards. It also demonstrates a commitment by the Association to process information in line with relevant legislation and codes of practice.

1.2.i This policy applies to all Association employees, board and committee members, temporary staff, contractors and agency workers, work experience students and volunteers who have authorised access to the Association's IT systems and premises. Everyone is expected always to protect the Association's IT systems and equipment from unauthorised access and harm and act in a way consistent with the protection of sensitive data outlined in the Data Protection Policy. Failure to do so may be dealt with under our Disciplinary Policy and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

1.2.ii This policy applies to:

- all devices used for business purposes including but not limited to laptops, desktop computers, mobile phones, tablets or other electronic equipment;
- all data, including but not limited to, electronic information found in emails, databases, applications and other media, and paper information found in hard copies of electronic data, files, internal memos and legal documentation; and
- information outside of the organisation stored in a cloud service and/or held on a mobile device.

1.3 This policy sets out how the Association manages the retention of information, records and data held by it and how it will:

- Improve its information management practices;
- Comply with current statutory, legal and regulatory requirements on retention of information and data protection;
- Implement archiving practices retaining archive records and retrieval systems;
- Minimise storage costs;
- Provide consistency for the management, archiving and disposal of information; and
- Improve operational efficiency.

1.4 This policy does not form part of any employee's contract of employment and it may be amended at any time.

2. Definition

2.1 The International Standard ISO/IEC 27001:2022 standard specification for Information Security Management defines Information Security as protecting three aspects of information:

- Confidentiality – making sure that information is accessible only to those authorised to have access.
- Integrity – safeguarding the accuracy and completeness of information and processing methods.
- Availability – making sure that authorised users have access to information and associated resources when required.

2.2 The Association holds a wide range of information about its services, activities, partners, employees, volunteers, residents and students and this is held both electronically and in hard copy. Information comes in many forms and can be:

- Stored on computers
- Sent across networks
- Printed out
- Written
- Spoken
- Visual.

2.3 Information Security covers the safeguarding of all forms of information to protect its confidentiality, integrity and availability both in its storage and disposal. In line with the Data Protection Act 2018 and its own Data Protection Policy, the Association will consider for disposal on a case-by-case basis information containing personal data that it no longer requires once any applicable statutory or regulatory retention period has lapsed and limitation periods have been considered.

2.4 This is put into practice through appropriate controls, which will be a combination of policies, procedures, standards, guidelines, common sense and physical or hardware/software measures.

3. Responsibilities and Accountabilities

3.1 The Chief Executive has responsibility for defining and setting the Association's Information Security policies, standards and procedures.

All management staff have a specific responsibility for operating within the boundaries of this policy, ensuring that all employees they manage understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

Every IT system user who has access to Association information is responsible and accountable for putting into practice those policies, standards and procedures. Information Security is not an option. Everyone is required to maintain at least a minimum level of security to meet the Association's legal and

contractual obligations. Day to day responsibility lies with the Head of Property Services.

Each service area of the organisation will be responsible for reviewing the information it holds, the purpose for holding it, ensuring it is accurate and up to date, and that information is held and disposed of responsibly. When a document has reached the end of its recommended/legal retention period, the relevant Head of Service/Director will authorise its disposal, subject to checking that the information is no longer needed.

Each department is responsible for completing its own data retention schedule which describes what information is held, the retention period and who is responsible for review and disposal of information that is no longer required to be held by the Association. A list of the retention schedules across the organisation is shown at Appendix 2.

All employees are responsible for adhering to this policy and will be required to sign and acknowledge that they have read and understood it. As an employee, if you are aware of any misuse of the Association's IT systems and equipment you should report this to your line manager or People Services. Questions regarding the content or application of this policy should be directed to your line manager or People Services.

4. Compliance with Legal and Contractual Requirements including Equipment Security and Passwords

4.1 The Association has an obligation to make sure that all information systems and processes meet the terms of all relevant legislation and contractual requirements, including (but not limited to) the:

- Data Protection Act 2018
- UK General Data Protection Regulation (Regulation (EU) 2016/679)
- Copyright, Designs and Patents Act 1988 (CDPA)
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Human Rights Act 1998

4.2 Desktop personal computers and cabling for telephones or computer equipment should not be moved or tampered with without first consulting the Head of Property Services.

Passwords are unique to each user and must be changed regularly to ensure confidentiality. Passwords must be kept confidential and must not be made available to anyone else. For the avoidance of doubt, on the termination of employment (for any reason) employees may be requested to provide details of their passwords to their line manager or HR department and return any equipment.

Employees who have been issued with a laptop, mobile phone, or other electronic equipment must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such

equipment to ensure that confidential data is protected in the event of loss or theft.

Employees should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

The following actions are required to maintain confidentiality, integrity and availability:

- Everyone has a shared responsibility to make sure that personal information is only collected, used, stored and shared for the purpose it was provided.
- Make sure any requests for personal information are handled in accordance with data protection legislation and the Association's Data Protection Policy. Information should only be disclosed on a need-to-know basis. Always make checks on the identity of enquirers.
- Make sure printed or handwritten personal information is kept secure at all times.
- Make sure printed or handwritten personal information is disposed of in a secure manner.
- Never dispose of personal information in general waste.
- Never allow IT equipment allocated or used by you to be used by anyone other than as permitted by policy. If leaving a terminal unattended or leaving the office, you should lock your terminal or log off to prevent unauthorised users accessing the system or personal information held on it. Employees/volunteers/service users without authorisation should only be allowed to use terminals under supervision.
- Never share usernames and passwords. Never encourage others to use anyone else's personal ID and password to log into a PC, the network, individual system or email.
- Always ensure that any devices which are issued by the Association, such as mobile phones, are passcode protected and locked when not in use.
- It is a criminal offence under the Computer Misuse Act 1990 to access a computer system without authority to do so.
- Be aware that emails are not usually a secure method of sharing personally identifiable information external to the Association.
- To avoid introducing viruses into the Association network never open email attachments from unknown external sources.
- Make sure you set your passwords to at least the minimum standard required in each case. Keep them secure and change them regularly.
- Use methods of encryption which are appropriate and technologically available to the personal data being processed following an evaluation of risks associated with that data.
- Be careful about maintaining confidentiality when speaking in public places, e.g. when speaking on a telephone.
- Do not leave any sensitive or confidential information in any place where it is at risk (e.g. car boots, cafés).

4.3 Managers must also make sure that employees are aware of procedures required for the management of non-electronic information. This includes not leaving

paper files unattended, have a clear desk policy, locking paper files away and transporting paper files securely and not leaving them unattended.

5. Compliance with Systems and Data Security

5.1 The Chief Executive and Senior Leadership Team are responsible for monitoring compliance with this policy. If employees knowingly or recklessly fail to comply with this policy, other Association policies, procedures or guidelines, the Association may take appropriate action under the disciplinary procedure.

5.2 Should an employee become aware of an actual or potential information security incident, they must immediately contact their line manager and the Data Protection Officer (Compliance Manager).

5.3 The Association operates a virus protection firewall on the server and personal computers as appropriate. Such virus protection software must not be "turned off" by employees. Intentionally removing or disabling virus protection software could lead to disciplinary action being taken.

Employees should not delete, destroy or modify existing systems, programs, information or data which could have the effect of harming our business or exposing it to risk.

Employees should not download or install software from external sources without authorisation from the Head of Property Services. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files.

No device or equipment should be attached to our systems without the prior approval of the Head of Property Services. This includes any USB flash drive, MP3 or similar device or telephone.

We monitor all emails passing through our system for viruses. Employees should exercise caution when opening emails from unknown external sources or where, for any reason, an email appears suspicious. The Head of Property Services should be informed immediately if a suspected virus is received. We reserve the right to block access to attachments to emails for the purpose of effective use of the system and for compliance with this part of our policy.

Employees should not attempt to gain access to restricted areas of the network, or to any password-protected information unless specifically authorised.

Employees using laptops or Wi-Fi enabled equipment must be particularly vigilant about its use outside the office and take any precautions required against importing viruses or compromising the security of the system. The system contains information which is confidential to our business and/or which is subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

6. Use and misuse of IT equipment and systems

Internet facilities are provided by the Association as a business tool to enable its employees to enhance the efficiency of their work for the Association and may not be used for personal purposes except during official breaks.

Misuse or abuse of our email system or inappropriate use of the internet in breach of this policy will be dealt with under our Disciplinary Procedure. Employees are required to inform their Line Manager if they become aware of, or suspect, the Association's internet facilities are being misused. Misuse of the internet can constitute a criminal offence in certain circumstances.

Misuse of the email system or inappropriate use of the internet includes, but is not limited to, participating in online gambling or chain letters, or creating, viewing, accessing, transmitting or downloading any of the following material and will amount to gross misconduct (this list is not exhaustive):

- Pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);
- Offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our customers/partners;
- A false and defamatory statement about any person or organisation;
- Material which is discriminatory, offensive, derogatory or may cause embarrassment to others;
- Confidential information about us or any of our employees, customers, service users or partners (which you do not have authority to access);
- Any other statement which is likely to create any liability (whether criminal or civil, and whether for you or us); or
- Material in breach of copyright.

Any such action will be treated very seriously and is likely to result in summary dismissal.

Where evidence of misuse is found we may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in our Disciplinary Procedure. If necessary, such information may be handed to the police in connection with a criminal investigation.

The Association reserves the right to report any illegal violation to the appropriate authority as necessary. It is illegal to create, access, store, transmit or publish any material which falls into the following categories:

- National Security: Instructions on bomb-making, illegal drug production, terrorist activities;
- Protection of Minors: Abusive forms of marketing, violence, pornography;
- Protection of Human Dignity: Incitement to racial hatred, or racial hatred or racial discrimination, harassment;
- Economic Security: Fraud, instructions on pirating credit cards;
- Information Security: Malicious hacking;

- Protection of Privacy: Unauthorised communication of personal data, electronic harassment;
- Protection of Reputation: Libel, unlawful comparative advertising; or
- Intellectual property: Unauthorised distribution of copyrighted works e.g., software or music.

The above are non-exhaustive examples and are not to be strictly construed.

It is unacceptable to create, access, copy, store, transmit or publish any material which is considered to be obscene, vulgar, to irritate or waste the time of others, to be subversive or to the detriment of the Association.

When assessing whether material is unacceptable, each case will be dealt with fairly and consistently and be judged on its own merits, considering the individual circumstances.

Care should be taken when downloading information from the internet and the potential risks and benefits should be accurately assessed. Downloading software can present a danger, please be aware of the following:

- The software may contain a non-detected virus.
- The downloaded software may not be compatible with the host computer configuration.
- Invoking the software may produce unexpected results.
- The software may be subject to copyright/licensing restrictions.

Before downloading any software, advice should be sought from the IT support officer.

Anyone, or any employee aware of anyone, inadvertently accessing illegal or unacceptable material should report it to the Compliance Manager immediately. Failure to act promptly could result in disciplinary action.

7. Monitoring of Use of the Systems

Our systems enable us to monitor email and internet usage. For business reasons, and in order to carry out legal obligations in our role as an employer, monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

We reserve the right to retrieve the contents of messages or check searches which have been made on the internet for the following purposes (this list is not exhaustive):

a. To monitor whether the use of the email system or the internet is legitimate;
b. To find lost messages or to retrieve messages lost due to computer failure;
c. To assist in the investigation of alleged wrongful acts; or
d. To comply with any legal obligation.

8. Information Disposal

8.1 Personal and sensitive information must be disposed of securely. Employees should carry out regular housekeeping of business information in accordance with the General Data Protection Regulation principles and the Association's Data Protection Policy.

8.2 Paper information should be destroyed using the appropriate means, either through a confidential waste disposal service, suitable shredding machines or other forms of suitable disposal. This is particularly important when disposing of or destroying personal data. Where a third-party contractor is appointed to manage the disposal of information, the Association must assess the risk to ensure that the contractor has signed a written agreement to comply with data protection legislation.

8.3 Where a Data Protection Officer deems that information requires to be held for longer than the recommended and/or legal requirement, a clear rationale must be identified. In some cases, this may relate to disputes, complaints or legal claims.

9. Monitoring and Review of this Policy

9.1 The Association will review the content of this policy every two years or earlier if there are changes in legislation or because of a change in good practice.

Appendix 1

Email Etiquette and Content

Email is a vital business tool, but an informal means of communication, and should be used with great care and discipline. Employees should always consider if email is the appropriate means for a particular communication; correspondence sent by email should be written as professionally as any other documentation. Messages should be concise and directed only to relevant individuals. Our standard disclaimer as stipulated below should always be included:

'The views expressed in this email are personal and may not necessarily reflect those of YMCA Derbyshire, unless explicitly stated otherwise. This email, and any files transmitted with it, are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error, please notify me immediately. If you are not the intended recipient of this email, you should not copy it for any purpose, or disclose its contents to any other person. YMCA Derbyshire cannot accept liability for viruses that may be in this email. We recommend that you check all emails with an appropriate virus scanner.'

Malicious emails from hackers are an increasing problem. Viruses can be transmitted via email to many users at one time or systems locked down until released after payment of a 'ransom'. Emails from an unknown source should be deleted without accessing any attachments or links included. Care should be taken to ensure that all data sent or received is virus free.

Employees should ensure that they access their emails at least once every working day, stay in touch by remote access when travelling and use an out of office response when away from the office for more than a day. Employees should endeavour to respond to emails marked "high priority" within 24 hours.

Employees should not send abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory emails. Anyone who feels that they have been harassed or bullied or are offended by material received from a colleague via email should inform their Line Manager or the HR department.

Employees should take care with the content of email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Employees should assume that email messages may be read by others and not include anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain.

Email messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main server or using specialist software.

Employees who receive a wrongly delivered email should return it to the sender. If the email contains confidential information or inappropriate material (as described above) it should not be disclosed or used in any way.

Use of email for personal use is not allowed. Email addresses should only be given out for business purposes and should not be given to personal contacts.

No emails or attachments which are not work related should be downloaded.

The email facility should be treated as any other business medium. When using email it is important to remember the following points:

- Emails can be sent effortlessly, but their content can be highly damaging.
- Most emails are not formal media. However, in certain cases a hard copy will need to be retained.
- Do not send information that insults or harasses others.
- Users must ensure that all statements are correct – email is a form of publishing to which libel laws apply.
- Users must not abuse others, even in response to abuse directed at them.
- Users must not participate in chain or pyramid mail or similar schemes.
- Users must try to ensure that statements cannot be misconstrued.
- Emails can be read by third parties.
- Emails can be used in evidence.
- Emails can create binding contracts.
- Do not broadcast trivial information to large groups, this wastes server space, wastes the time of the recipients and can lessen the impact of important mail.
- The inappropriate use of upper case in email is generally interpreted as SHOUTING and should be avoided.
- Emails are not guaranteed to be private nor to arrive at their destination either within a particular time or at all.

Appendix 2

Retention Schedule for YMCA Derbyshire Services

Service	**Lead Responsibility**
GDPR	Kelly Jackson
Accommodation and Support Services	Wayne Exton
Training and Education • Key College • Adult Programmes	Louise Curd
Estates and Maintenance IT Operations	Phil Simpson
Finance	Andrew Armstrong
People Services	Kira Horvath
Conference Centre	Phil Simpson
Income Generation Marketing Bid Writing Youth and Community	Grace Harrison
Derwent Stepping Stones Y-Kidz	Janet Holland

Monitoring of the Retention Schedule and contents will be undertaken by a Data Protection Officer (Executive Director – Corporate Servies) with quarterly reports to the Senior Leadership Team and annual reports to the Board.