Community Bike Kitchen CiC

Reviewed 31.03.2025 reviewed every two years – next review 31.03.2027

Data Protection & Records Management Policy

Community Bike Kitchen CiC commitment to Records Management is expressed by its records management policy. This policy embraces all records of Community Bike Kitchen CiC actions and activities in whatever format they exist.

1 Responsibility for record keeping

In the context of this policy, those with responsibility for keeping and managing Community Bike Kitchen CiC records include those full-time and part-time members of Community Bike Kitchen CiC staff, centrally managed and seconded into regional roles. This policy will also cover office-based volunteers, who may from time-to-time support the work of Community Bike Kitchen CiC nationally.

2 Exclusions

2.1 This policy does not cover the records management of local projects within the Community Bike Kitchen CiC network or those contractors who may work on behalf of Community Bike Kitchen CiC.

2.2It is expected that local Community Bike Kitchen CiC projects and contractors will follow their own organisational policy guidance on the appropriate management and retention of records.

3 **Creation of Community Bike Kitchen CiC records**

3.1 Community Bike Kitchen CiC records will be created for a number of purposes including:

- Records of Human Resources matters relating to staff;
- Minutes of meetings and documentation relating to the running of the organisation;
- Financial records of transactions relating to income and expenditure;
- Records of activity for monitoring and evaluation purposes and in order to report to external funding bodies.

4 Storage of Community Bike Kitchen CiC records

4.1 There are a number of ways in which records can be kept including paper-based format, electronically on a server or computer hard-drive or on a device such as a USB memory stick.

4.2 In recognition of this range of storage methods Community Bike Kitchen CiC will adopt the following statements of principle for storage of records:

- That records containing the personal details of staff or project participants will be stored securely either through password protection electronically or through the use of lockable storage for paper-based records.
- That personal records will not be kept on unsecured media, such as a USB memory stick.
- That Community Bike Kitchen CiC staff will periodically review the records for which they have responsibility and retain or destroy them as appropriate.

5 Retention of records

5.1 Records should be destroyed at the right time. Some records need to be kept for periods specified by law whilst others are covered by authoritative best-practice codes. For many more, however, retention is simply a matter of operational need. In any case, **destruction is irreversible** and retention decisions must be made with an awareness of the following factors:

- The requirements governing record-keeping by charitable organisations;
- The requirements of external funding bodies for record retention relating to funding bids;
- The operational benefit of retaining records e.g. for planning future activity;
- The future need for personal records e.g. for writing references for staff.

5.2 In cases of uncertainty, Community Bike Kitchen CiC staff will be encouraged to refer to the Director of Finance and Operations for guidance.

5.3 In line with best practice, the retention period for a record should be decided at its creation and records should also be appropriately dated.

5.4 Records should be destroyed in an appropriate manner. As many Community Bike Kitchen CiC records may contain sensitive personal information secure destruction (e.g. through shredding or confidential waste for paper records) is always recommended.

6 Document Retention Schedule

6.1 To assist staff within the organisation with the appropriate management of records relating to Community Bike Kitchen CiC work, the Director of Finance and Operations may choose to employ the use of a Document Retention Schedule (see Appendix 1).

Appendix 1

Nature of Record	How Long Kept?	Action at the End of that Period	Relevant Legislation (if any)	**Reason** eg, statutory requirement, best practice, audit, operational need
1 Administration (This section relates only to records which do not form part of a specific service or matter)				
Distribution Lists	Until updated	Destroy		Operational need
Databases	Until updated	Destroy		Operational need
General Administrative Records	Until no longer relevant	Destroy		Operational need
Spreadsheets	Until no longer relevant	Destroy		Operational need
Team Meetings	3 years	Destroy		Operational need
Websites - Working documents	3 years	Destroy		Operational need
2 Strategy & Performance				
Service Plans	Until updated/amended	Destroy		Operational need
Disability Audit	Until next audit	Destroy		Operational need
Documents relating to Equality Development	Until no longer relevant or replaced	Destroy		Operational need
Performance Indicators	Until no longer relevant or replaced	Destroy		Operational need

Community Bike Kitchen CiC

3 Key Projects

Project Documentation	2 years after completion of project	Archive if major project, otherwise destroy		Audit
Project Management Documentation	2 years after completion of project	Destroy		Operational need
Project Budget Documentation	2 years after completion of project	Destroy		Audit
Project Outputs	Retain as appropriate for output			Audit

4 Budget & Finance

Banking Records	3 years or, if storage space is a problem, at least until accounts are signed off by external audit for the year in question .	Destroy		Audit
Budget Notes & Working Papers				
Budget Monitoring				
Cash Collections & Petty Cash				
Debtors & Credit Documents				
Expenditure				
Internal Transfer				
Reconciliations				
Paid Invoices	7 years retain with CB	Destroy		VAT and Legal

Payroll Records				

5 European Funded Projects

Receipts, Invoices and project management documentation	Project contract specifies the date at which documentation can be destroyed.	Review Destroy		

6 Purchasing - Minor Contracts - Below £50,000

Quotes	Length of contract plus 1 year or longer as determined by warranty	Review/Destroy		
Contract Management				
Contract Documentation				
Purchase Orders	1 year or longer as determined by warranty	Review/Destroy		
Stock Information	1 year	Review/Destroy		
Goods Received	Retained until receipt of invoice	-Review/Destroy		
Delivery Notes				

Unsuccessful tenders	18 months after all the following have happened or been considered: a)all payments under the contract have been made b) all of the requiremetns under the terms of the Contract have been succesfully carried out, and c) they are not likely to be required for inspection by external auditors	Destroy		

7 Audit Records

External Audit	6 years	Review/Destroy		Audit

8 Complaints

Complaints Files Complaint Letters Investigation reports Ombudsman correspondence	3 years from final decision letter to complainant	Destroy		Operational need

9 General Correspondence (not held as part of another file ie contract documentation)

Correspondence with Customers, letter/email/web	1 year but do not keep e-mails on PC/Laptop. If necessary, put hard copy on file.	Destroy		Operational need

Correspondence Enquiries				

Community Bike Kitchen CiC

10 Personnel

Personal Files Containing:-

Completed Appraisal Documents	In general individual Personal Files should be kept for 6 years from termination of employment	Review/Destroy		Legal
Health & Safety Records				
Job Descriptions				
Miscellaneous				
Recruitment Details				
Sickness Details				
Timesheets				
Training Records				
1 to 1 Notes	Keep for a minimum of 2 years, or longer if the individual is subject to ongoing capability management			Operational Need
Hours	2 years			
Rotas				
Holiday Details	End of following leave year			

Disciplinary Files

Disciplinary Reports	15 months or longer if the review period is set at a longer period	Review/Destroy		Legal/Operational
Disciplinary Findings				

Community Bike Kitchen CiC

General Staff Information

Accident records	25 years for health& safety and occupational health records. Six years for the rest	Review/destroy		Legal/Operational
Health and Safety records				
Occupational Health records				
Policies and procedures	6 Years			
General Training Records				
General Sickness Records	Until updated			
Rotas	6 Months			

Health & Safety*

Risk Assessments	7 years.	Review/Destroy		Legal/Operational
Site Inspection Records				
Local Safety Practices				
Accident Statistics				
Asbestos Management Records	Permanently			

* If people have been accidently exposed to high levels of asbestos or chemicals then relevant risk assessments, policies, procedures, inspection reports, health surveillance etc needs to be retained.

Community Bike Kitchen CiC

Removable Media Controls

1.0 Overview

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations.

2.0 Purpose

The purpose of this policy is to minimize the risk of loss or exposure of sensitive information maintained by Community Bike Kitchen CiC and to reduce the risk of acquiring malware infections on computers operated by Murray State Community Bike Kitchen CiC. Any questions or comments about this policy should be directed to Information Systems.

3.0 Scope

This policy covers all removable media that contains Community Bike Kitchen CiC data or that is connected to a Community Bike Kitchen CiC network.

4.0 Policy

Community Bike Kitchen CiC staff may use removable media in their work computers. Sensitive information should be stored on removable media only when required in the performance of assigned duties or when responding to legitimate requests for information. When sensitive information is stored on removable media, it must be encrypted in accordance with the Community Bike Kitchen CiC Acceptable Encryption Policy. Exceptions to this policy may be requested on a case-by-case basis by petition to Information Systems.

5.0 Enforcement

Anyone found to have violated this policy may be subject to disciplinary action, up to and including suspension of access to technology resources or termination of employment. Students may be referred to Student Affairs for discipline. A violation of this policy by a temporary worker, contractor or vendor may result in action up to and including termination of their contract or assignment with Murray State Community Bike Kitchen CiC.

6.0 Definitions

Removable Media

Removable media is defined as devices or media that is readable and/or writable by the end user and are able to be moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, SD cards, cameras, MP3 players and PDAs; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; floppy disks and software disks not provided by Murray State Community Bike Kitchen CiC.

Encryption

Encryption is a procedure used to convert data from its original form to a format that is unreadable and/or unusable to anyone without the tools/information needed to reverse the encryption process.

Malware

Malware is defined as software of malicious intent/impact such as viruses, worms, and spyware.

Community Bike Kitchen CiC Network

Being connected to a Community Bike Kitchen CiC network includes the following:

- If you have a network capable device (ex. laptop) plugged into a Community Bike Kitchen CiC owned building, then you are connected to the MSU LAN (local area network).
- If you have a wireless capable device (ex. laptop, iPhone) and connect to MSU Wireless or MSU Secure, then you are connected to the MSU WLAN (wireless local area network).
- If you connect from a computer through the Community Bike Kitchen CiC VPN (virtual private network), you are then connected to the MSU LAN (local area network).

Sensitive Information

Sensitive information is defined as information which, if made available to unauthorized persons, may adversely affect Murray State Community Bike Kitchen CiC, its programs, or participants served by its programs. Examples include, but are not limited to, personal identifiers and financial information. The determination of sensitivity is the responsibility of individual departments.

Mobile and Remote Working Policy

1. Introduction

This Mobile and Remote Working policy is a sub-policy of the Information Security policy (ISP-01) and sets out the additional principles, expectations and requirements relating to the use of mobile computing devices and other computing devices not located on Community Bike Kitchen CiC premises when devices are used to access Community Bike Kitchen CiC data.

While recognising the benefits to the Community Bike Kitchen CiC (and its members) of permitting the use of mobile devices and working away from the office, the Community Bike Kitchen CiC also needs to consider the unique information security challenges and risks that will necessarily result from adopting these permissive approaches. In particular, the Community Bike Kitchen CiC must ensure that any processing of personal data remains compliant with UK Data Protection legislation.

2. Scope

This policy applies to all members of the Community Bike Kitchen CiC and covers all mobile computing devices whether personally owned, supplied by the Community Bike Kitchen CiC or provided by a third party. Personally owned, Community Bike Kitchen CiC owned or third party provided non-mobile computers (for example desktops) used outside of Community Bike Kitchen CiC premises are also within scope.

2.1. Definitions

A mobile computing device is defined to be a portable computing or telecommunications device that can be used to store or process information. Examples include laptops, netbooks, smartphones, tablets, USB sticks, external or removable disc drives, flash/memory cards and wearable devices and smart devices.

Community Bike Kitchen CiC data is classified as any data belonging to the Community Bike Kitchen CiC. This includes emails, office documents, database data, personal and financial data. Data obtained from third parties, including research and clinical data obtained under a data sharing agreement with the Community Bike Kitchen CiC, would also be considered Community Bike Kitchen CiC data.

3. Policy

3.1. Personally owned devices

Whilst the Community Bike Kitchen CiC does not require its staff or postgraduate researchers to use their own personal devices for work purposes, it is recognised that this is often convenient and such use is permitted subject to the following minimum requirements and guidelines. Users must at all times give due consideration to the risks of using personal devices to access Community Bike Kitchen CiC data and in particular, information classified as confidential or above:

- The device must run a current version of its operating system and must also have a recent security update installed. A current version is defined to be one for which security updates continue to be produced and made available to the device.
- Mobile devices must be encrypted.
- An appropriate passcode or password aligned with the Community Bike Kitchen CiC's password guidance, must be set for all accounts which give access to the device. The use of biometric authentication methods is also acceptable.
- A password protected screen saver/screen lock must be configured.
- The device must be configured to “autolock” after a period of inactivity (no more than 15 minutes).
- Devices must remain up to date with security patches both for the device’s operating system and its applications.
- Devices that are at risk of malware infection must run anti-virus software.
- Software firewalls must not be disabled or updates postponed. Devices capable of employing a software firewall will typically have this enabled by default and set to automatically update.
- All devices must be disposed of securely, including the removal of Community Bike Kitchen CiC data before disposal, in accordance with the Disposal of Information section of the Community Bike Kitchen CiC's policy.

- The loss or theft of a device must be reported to IT Services.
- Any use of personal devices by others (family or friends) must be controlled in such a way as to ensure that these others do not have access to Community Bike Kitchen CiC data classified as Confidential or above.

In addition to the minimum requirements above, the following recommendations will help further reduce risk:

- Consider configuring the device to “auto-wipe” to protect against brute force password attacks where this facility is available.
- Consider implementing remote lock/erase/locate features where these facilities are available.
- Do not undermine the security of the device (for example by “jail breaking” or “rooting” a smartphone).
- Do not leave mobile devices unattended where there is a significant risk of theft.
- Be aware of your surroundings and protect yourself against “shoulder surfing”.
- Minimise the amount of restricted data stored on the device and do not store any data classified as confidential or above.
- Access restricted information assets via the Community Bike Kitchen CiC’s remote access services (see page http://www.bristol.ac.uk/it-services/advice/homeusers/remote/ for more information) wherever possible rather than transferring the information directly to a device.
- Be mindful of the risks of using open (unsecured) wireless networks. Consider configuring your device not to connect automatically to unknown networks.
- If a personally owned device needs to be repaired, ensure that the company you use is subject to a contractual agreement which guarantees the secure handling of any data stored on the device.
- Reduce the risk of inadvertently breaching UK Data Protection legislation by ensuring that all personal data pertaining to Community Bike Kitchen CiC business, which is subject to the legislation and is stored on the device, is removed before taking the device to a country outside of the European Economic Area.

3.2. Community Bike Kitchen CiC owned devices

The Community Bike Kitchen CiC may at times provide computing devices to some of its members. When it does, it will supply devices that are appropriately configured so as to ensure that they are as effectively managed as devices that remain within the office environment.

Devices supplied by the Community Bike Kitchen CiC must meet the minimum security requirements listed above for personally owned devices.

In addition, the following are required:

- Non-members of the Community Bike Kitchen CiC (including family and friends) must not make any use of the supplied devices.
- No unauthorised changes may be made to the supplied devices.
- Devices assigned to a specific user should only be used by that user.
- All devices supplied must be returned to the Community Bike Kitchen CiC when they are no longer required or prior to the recipient leaving the Community Bike Kitchen CiC, irrespective of how they were purchased (for example, grant funding).

3.3. Third party devices

On occasion, staff and research postgraduates may be supplied with computing devices by third parties in connection with their research. These devices must be effectively managed, either by the third party, by the Community Bike Kitchen CiC or by the end user. In all cases, the device must meet the minimum security requirements listed above for personally owned devices.

3.4. Remote working environment

When working remotely (either at home or elsewhere), steps must be taken to secure your working environment. In particular, where possible default passwords must be changed for all devices (including personal mobile devices accessing Community Bike Kitchen CiC data and wi-fi routers).

Accessing data classified as confidential on publicly available devices or networks should be avoided. Data classified as confidential and sensitive or above must not be accessed on publicly available devices or networks. Publicly available devices and networks include shared computers and wireless networks in public libraries, hotels, and cafés or restaurants. When accessing data classified as confidential or above on public networks, a Community Bike

3.5. Reporting losses

All members of the Community Bike Kitchen CiC have a duty to report the loss, suspected loss, unauthorised disclosure or suspected unauthorised disclosure of any Community Bike Kitchen CiC information asset to the information security incident response team (info@communitybikekitchen.co.uk).