Gloucestershire Archives @ The Hub

Buildings and Collections Security Policy

1. Policy statement and purpose

Gloucestershire Archives aims to ensure that the collections in its care are kept securely and preserved permanently.

To this end, we seek to reduce the risk of damage or loss to our collections through accident or deliberate act by taking all measures necessary within our resources. The purpose of this policy is to explain the security framework within which we operate.

2. Scope

This policy applies to the physical security of the collections in our care in relation to

- Site and buildings
- Strong rooms and document storage areas
- Public areas
- Staff and volunteers
- Contractors and visitors
- Transport of collections
- Temporary withdrawals from collections
- Data about collections management

The security of digital collections is covered separately by the Digital Preservation Policy (see section 14, References). Wider information security, data protection and digital, information and communications technology (DICT) controls are governed by Gloucestershire County Council policies.

Equality, diversity and inclusion: Security arrangements will be implemented proportionately and in ways that support equitable and inclusive access. Reasonable adjustments will be considered so that security procedures do not create unnecessary barriers for customers, volunteers, staff or other visitors.

3. Terminology

Archives are the record of everyday activities of governments, organisations, businesses and individuals. Archives may take many different forms – handwritten, typed, printed, photographic or electronic – and include audio-visual material such as video and sound recordings. As authentic and reliable records, they are preserved permanently because of their evidential and historical value.

Local and family history resources comprise published information about the history of local areas and their communities, for example, newspapers and locality-based books, pamphlets and journals covering a wide range of topics.

4. Background

Gloucestershire Archives gathers archive collections and local and family history resources to ensure they are kept secure and made accessible.

We are an accredited archive service recognised by The National Archives as the place of deposit for Public Records relating to Gloucestershire and South Gloucestershire.

We operate as a Gloucestershire County Council service. By agreement, we also provide an archive service for South Gloucestershire Council and are the appointed Record Office for the Diocese of Gloucester.

Gloucestershire Archives is a lead partner in the Gloucestershire Heritage Hub, a network of local people and organisations with a common interest in our historic county's documented heritage.

5. Security of site and buildings

Our service operates from the Heritage Hub site at Kingsholm, Gloucester.

Site and building security are a service priority. Advice is taken from security and fire-prevention specialists before major alterations or new building works. All staff receive appropriate security and emergency-preparedness training and are expected to report suspicious behaviour or objects. The service falls outside the scope of the Terrorism (Protection of Premises) Act 2025, commonly known as Martyn's Law, but has created a procedure and regularly reviews lockdown arrangements and training.

Measures are in place to control access to the site and prevent unauthorised entry to the buildings. Door-access controls are programmed and fully auditable, and the Head of Archives Service carries out periodic checks of access-control data. A planned inspection and maintenance programme covers the site, buildings and installations, including boilers, intruder alarms, CCTV, fire-detection systems and fire-extinguishing equipment.

Any actual or suspected theft, loss, unauthorised access, malicious damage, data compromise or other security incident must be reported immediately and escalated through the relevant service and Gloucestershire County Council procedures. Evidence and access-control records will be preserved where appropriate; owners or depositors and relevant GCC services, emergency services or insurers will be notified as required. Incidents will be reviewed and corrective actions recorded, with reference to the service's business continuity, emergency response and collections salvage arrangements.

6. Security of strongrooms and document storage areas

Our strongrooms are equipped for fire prevention and detection, protection against flooding and prevention against unauthorised intruders. They are designed to ensure that temperature and humidity levels meet national standards for archive storage (see section 14, References).

Only staff (and occasionally volunteers, visitors or authorised contractors accompanied by staff) may access the strongrooms. They are kept secure at all times except when access is required.

Documents may be stored temporarily in sorting or cataloguing rooms but are moved into strongrooms as soon as possible.

Procedures and training are in place to prevent accidental misplacement of records or damage to collections occurring through poor storage and mishandling.

7. Security in public areas

We are committed to providing good access for visitors while ensuring the security of our collections. Measures are in place in the public research room to control and supervise access and to prevent theft, malicious or accidental damage and misplacement. Rules are displayed prominently on research room tables.

There are additional arrangements to control access to confidential records.

8. Security in relation to staff and volunteers

Staff are appointed once satisfactory references have been obtained and their employment is confirmed only after they have successfully completed a probationary period. Similarly, some volunteering roles also require references and agreed standards of conduct to be met. All volunteers with access to collections are supervised by staff.

Staff are trained in security, response to terrorism, and fire procedures and in the safe and careful handling of collections, appropriate to their roles and responsibilities. Failure to comply with procedures will lead to disciplinary action or the end of a volunteering agreement.

9. Security in relation to contractors and visitors

Contractors: The Buildings and Collections Security Officer maintains a register of permits for contractors and supervises their work. No contractor is allowed on site without signing the register. No contractors are permitted to work in the strongrooms unsupervised by staff.

Other visitors: The relevant member of staff hosting a visit takes responsibility for correctly signing visitors into the building and accompanying and supervising visitors in staff-only areas. Customers and volunteers using the research room, by appointment only, are required to sign up to the Archives and Records Association's (ARA) Archives Card scheme at https://www.archivescard.com/ to ensure document security on this site and all other sites in the national scheme. Each time an online document request form is submitted, customers must also agree to following research room rules as part of the appointment process.

10. Security during transport of collections to the Archives

Owners are encouraged wherever possible to transport their collections in person. If the owner is unable to transport their collection, then staff may offer to transport smaller collections directly (for example, on way from home to work) and a signed receipt will be given to the owner. The collection will not be left unattended.

Where direct transport is not appropriate, a removal firm experienced in handling archives may be used. Any alternative arrangement must be agreed in advance with the owner and Collections Management staff and must meet the same requirements for documentation, handling, security and insurance. The library van system may be used to transfer stock from libraries.

11. Security during temporary withdrawals of records from the Archives

Withdrawals of records can only be made by the owner or with the written permission of the owner; a record is kept of show requested the withdrawal, the date of withdrawal and the return.

Requests for temporary withdrawals are dealt with by the Collections Management Team. Reasonable notice is required and a return date must be agreed. A condition check will be completed where appropriate, and advice on safe handling, security and transport will be provided. Records remaining withdrawn beyond the agreed date will be monitored and followed up.

In exceptional instances, Items from collections may be taken off site by staff only with appropriate authorisation and, where required, the owner's permission. Examples of such instances include Public Inquiries, displays or other staffed events, or short-term temporary displays in museums with appropriate security and environmental conditions and insurance arrangements.

Digital copies in place of original archive material are used whenever possible for off-site Archives outreach activities.

12. Security of collections management data

Data relating to the provenance, ownership, quantity and content of collections are recorded at the time of transfer to the Archives. Information about collections is recorded systematically. This includes work undertaken on collections, such as appraisal, disposal, physical arrangement, storage and conservation.

All data is maintained, updated in a timely way, and stored securely in our collections management database. Legacy paper records and other digital records relating to collections management (for example, correspondence with owners of archives) are also stored securely. Recovery arrangements are in place for all data. Staff are trained in cyber security through regular and comprehensive online training packages provided by Gloucestershire County Council.

13. Roles and responsibilities

Day-to-day site security and building maintenance are the responsibility of the Buildings and Collections Security Officer, reporting to the Head of Archives Service. Systems are

checked daily or weekly as needed by the Buildings and Collections Security Officer or a nominated deputy.

Day-to-day collections security is the responsibility of all Archives staff but in particular the Collections Team working under the direction of the County Archivist. All staff have a responsibility to complete the cyber security training provided and to be aware of risks.

The Head of Archives Service and the Archives Management Team are responsible for arranging appropriate training, ensuring compliance and following up identified actions.

Day-to-day data systems security and data recovery is the responsibility of Gloucestershire County Council's DICT team. Cyber security training is delivered by the Information Management Service.

14. References

This policy should be read alongside the service's Collections Care, Access, Digital Preservation and Collections Development policies available at www.gloucestershire.gov.uk/archives/policies. This policy is supported by documented and practiced business continuity, emergency planning and collections salvage arrangements.

Gloucestershire County Council's policies for Information Security and Data Protection can be found at www.gloucestershire.gov.uk/council-and-democracy/strategies-plans-and-policies/information-management-and-security-policies/information-and-data-management-policies/

Supporting standards:

- BS EN 16893:2018, Conservation of cultural heritage — Specifications for location, construction and modification of buildings or rooms intended for the storage or use of heritage collections
- BS 4971:2017, Conservation and care of archive and library collections
- Terrorism (Protection of Premises) Act 2025 and current statutory guidance
- Benchmarks in Collections Care 2.0, Museums, Libraries and Archives Council, 2011
- Archive Service Accreditation Standard and current supporting guidance

15. Review and revision

This policy will be reviewed every three years, or earlier following a significant security incident, material change in risk, relevant legislative change or updated statutory guidance. Please write to archives@gloucestershire.gov.uk if you wish to give feedback on this policy.

Document Control

Author:	Julie Courtenay, former Collections Leader; Heather Forbes, Head of Archives Service
Owner:	Heather Forbes, Head of Archives Service
Approval Body	Gloucestershire Archives Management Team (GAMT); Gloucestershire County Council's Director of Policy, Performance & Governance; South Gloucestershire Archives Liaison Group
Date Approved	TBC
Document Number:	V2.5

Version History

Version	Version date	Summary of Changes
1.1	Jan 2010	Policy approved by Libraries Senior Management Team
2.0	July 2014	Policy reviewed and minor revisions approved by GAMT
2.1	Sept 2014	Brief review and minor re-formatting
2.2	Dec 2017	Review following restructuring of service
2.3	Oct 2020	Supporting standards and job titles updated; visitor and contractor security arrangements updated; paginated.
2.4	Oct 2023	Review with standards and links updated; training provision enhanced in light of Martyn's Law and increased cyber-security risks.
2.5	Oct 2026	Updated with inclusive access, Martyn's Law section revised, risk and incident management, job title and supporting standards

Date of next revision: 2029

After consultation add back the original footer.