Revised 13 November 2020

XXXXX

Historic Environment Record
Data Management Statement (DMS)

Author(s):	xxxxxx
Origination Date:	2 November 2020
Reviser(s):	
Date of last revision:	
Review due:	Annually
Version:	1
Status:	Draft
Summary of changes:	
File name/location:	I:\Public Protection & Culture\Heritage and Tourism\Archaeology\AR7.0.0 HER\AR7.4.0 Policies&Manuals\HER Policies and Plans
Authorities covered by the HER:	xxxx

Related policies:	Date of last revision	Revision required	Review Cycle	Location
Systems Security Policy Recording Policy Disposals Policy Disaster Recovery Plan Business Continuity Plan	October 2020	October 2021	Annual	I:\Public Protection & Culture\Heritage and Tourism\Archaeology\AR7.0.0 HER\AR7.4.0 Policies&Manuals\HER Policies and Plans\ WBC_HER_Policies_2020
Recording Manual	October 2018	October 2020 (overdue)	Annual	I:\Public Protection & Culture\Heritage and Tourism\Archaeology\AR7.0.0 HER\AR7.4.0 Policies&Manuals\HER Recording Manual\DataentryManual_HBSMRv5
Index to Reference Collection	November 2020	Ongoing	Ongoing	I:\Public Protection & Culture\Heritage and Tourism\Archaeology\AR1.0.0 Archaeology (general)\AR1.5.0 Our resources\2020 Archaeology Service resources
Prioritised list of backlog	October 2020	Ongoing	Ongoing	I:\Public Protection & Culture\Heritage and

<table>
<tr><td>List of Enhancements</td><td>Ongoing</td><td>Ongoing</td><td>Ongoing</td><td>Tourism\Archaeology\AR1.0.0 Archaeology (general)\AR1.10.0 Statistics\StatisticsCurrent\Current_ReportsReceived
I:\Public Protection & Culture\Heritage and Tourism\Archaeology\AR7.0.0 HER\AR7.9.0 Enhancement\xxxx</td></tr>
<tr><td><em>Does the HER manage any other databases that have not been fully integrated into the main HER e.g. UAD, HLC, legacy database)?</em></td><td colspan="4">If yes, please detail here: HLC is a standalone GIS layer, partly integrated into HBSMR. Relevant files can be found in I:\Public Protection & Culture\Heritage and Tourism\Archaeology\AR4.0.0 Projects\AR4.1.0 Historic_Landscape_Characterisation\our_hlc.</td></tr>
<tr><td colspan="5"><strong>Contact HIPsTeam@HistoricEngland.org.uk if you have any queries when completing this form.</strong>
<strong>Please send your completed form, Part A (signed) and Part B, to HIPsTeam@HistoricEngland.org.uk</strong></td></tr>
</table>

This Data Management Statement forms part of the Heritage Information Access Strategy (HIAS) ***National Security Copy Code of Practice*** (NSC CoP).

The Code covers two main types of security copying:

1. Consistent routine backups where security copies are made of a heritage dataset by an organisation (covered by the **Data Management Statement**, CoP Part 1).
2. Exceptional decisions to deposit a security copy with another heritage organisation for safeguarding (covered by the **Access Protocol**, CoP Part 2).

The DMS:

- Provides information needed to recover data and systems following a disaster, accident or other disruption to the HER service;
- Identifies and defines the roles and responsibilities of those involved in backups and data security;
- Confirms relevant staff are informed about secure data handling and backups;
- Identifies (or signposts existing documentation containing details of) any copyright in the data or access licences;
- Identifies (or signposts existing documentation containing details of) any legal restrictions or statutory regulations which affect deposit of the data (e.g. personal or confidential data);
- Is an overarching document that refers to related standard HER policies where these have been completed by the HER.

When the Access Protocol is invoked, the DMS should be included in the supporting documentation accompanying the data being deposited.

Historic England will coordinate each year a number of rehearsals of the process to prepare a security copy and test its effectiveness. You may be invited to participate in a rehearsal as part of the annual monitoring of NSC compliance.

Part A

The HER system and software

Give a brief description of the systems and software that you use. Describe who developed the system and how it is maintained. Please supply a link or reference to relevant documentation, including licences.

The HER includes textual data in a computerised database using HBSMR v5.50.12, which is linked by MapLink 6.2.3631 to spatial data in digital form on a Geographic Information System (GIS) using ArcGIS Desktop 10.5.1.

HBSMR is an off-the shelf software package developed and supplied under licence by Exegesis Spatial Data Management Ltd (licence numbers xxx). It stores data in an SQL Server database at xxxx offices and uses Access for the user interface.

The GIS layers are stored on an SQL Server database specific to the HBSMR application, also at xxx offices. Most layers are not part of a corporate GIS layer, but some are displayed on the Council's online map, intranet map, as a corporate layer in ArcMap and on Heritage Gateway. It has Ordnance Survey data supplied under licence number xxx.

Programme components are installed on Citrix.

General ICT support is provided by the IT Helpdesk, which can be contacted on xxx

Specialist support for the GIS software is provided by GIS Application Support Officer, Chris Matthews, who can be contacted on xxx.

Licences required include: HBSMR, HBSMR Consultations module, LibraryLink, ArcGIS, MapLink, Ordnance Survey, Landmark Information Group and Microsoft Office.

Data

Please provide a top-level, overview description of the data held.

Data Type	Range of formats involved	Volume/File size	Location	Existing metadata** /catalogue?
Database	SQL server database	c. 850 MB	On-premises SQL Server	Yes (HBSMR Audit Trail)
GIS Layer	SQL server database	c. 702 GB	On-premises SQL Server	Yes (HBSMR Geographic

				Position metadata)
Linked digital files	PDFs, xls, tiff, jpeg, doc	c. 50.4 GB	J:\Access\ESDMLibLinkFiles\HBSMRLibLinkFiles	Yes (HBSMR Source Record and Audit Trail)
Stand-alone digital files, including NMP data*	PDFs, xls, tiff, jpeg, doc. NMP files are of two types – Raster (an image) and Vector, both from aerial photographs	c. 55.2 GB	J:\Access\ESDMLibLinkFiles\HBSMRLibLinkFiles (for grey literature and images) and I:\Public Protection & Culture\Heritage and Tourism\Archaeology\AR5.0.0 Planning (for Consultation documents)	Yes (HBSMR Source Record, Consultation Record and Audit Trail)
Paper-based information sources	Site-specific paper files, aerial photographs, other printed photographs, microfiche, slides, grey literature not yet digitised, library books and offprints	Four cupboards	See spreadsheets in I:\Public Protection & Culture\Heritage and Tourism\Archaeology\AR1.0.0 Archaeology (general)\AR1.5.0 Our resources\2020 Archaeology Service resources and I:\Public Protection & Culture\Heritage and Tourism\Archaeology\AR1.0.0 Archaeology (general)\AR1.10.0 Statistics\StatisticsCurrent\Current_ReportsReceived	Yes (HBSMR Source Record, Audit Trail and Archaeology Service resources list)

*For example, may include NMP, HLC, UAD, EUS data not integrated into the HER system, digital grey literature PDFs etc. These may be located on servers or stored on external media such as CDs, HDDs.

** Metadata to accompany each of the digital and non-digital components of the HER should include as a minimum: file name, file type, description of the data and purpose, date of creation, date of last update, origin, restrictions of use, and rights information. Advice on the creation of metadata can be found at https://archaeologydataservice.ac.uk/advice/guidelinesForDepositors.xhtml; www.ukdataservice.ac.uk/manage-data/document/metadata.aspx and www.agi.org.uk/agi-groups/standards-committee/uk-gemini.

Digital data backup

Back up procedures:

Please fill in the table below regarding backups for the HER database, GIS, digital reference collection and system files (where relevant). If an option doesn't suit your arrangements you can add your own text.

	Backups made?	Type of Backup	Backup frequency	No. of copies	Backups retained for
HER and GIS Data	Yes	Complete	Daily	3	Daily – 2 weeks Weekly – 8 weeks Monthly – 1 year
Digital Ref. Collection	Yes	Complete	Daily	3	Daily – 2 weeks Weekly – 8 weeks Monthly – 1 year
System Files	Yes	Incremental	Daily		1 year

Additionally, please explain who is responsible for making the backups and where they are stored. Please detail for both the data and the system files (where relevant e.g. if bespoke software).

The Server and Storage Team looks after all the backups of all of the Council's systems. The team runs incremental backups daily and full backups on the weekends with the last weekend of the month going off site to a third party vault. All backups are stored initially locally on disc, then on tape at the Council's xxx office, then on tape offsite. The maintenance and backups of the Council's SQL Server estate is the responsibility of the Council's Senior Database Administrator. Full SQL Server backups are taken on a daily basis (and where appropriate transactional backups are taken at 30 minute intervals between these). These backups are written to disc and subsequently backed up to tape as part of the server level backups. Backups are retained on disc for three days for immediate recovery purposes. For the restoration of older backups, they are initially restored from the server backup tapes before being restored to reconstitute the required database.

Testing back up procedures:

Please fill in the table below regarding backup testing and recovery for the HER database, GIS, digital reference collection and system files (where relevant).

	Regular data recovery tests?	Backup copies monitored/ examined?	Successful recovery from backup?	Loss or corruption of data/files past two years?
HER Data	Yes	Yes	Yes, complete	No
GIS Data	Yes	Yes	Yes, complete	No
Digital Ref. Collection	Yes	Yes	Yes, complete	No

System Files	Yes	Yes	Yes, complete	No

Please keep a log of any recovery tests, incidents of lost or corrupted data/files in Appendix 1 as part of the DMS.

Please give details of the criteria you use in the testing process. Are procedures for data recovery adequately documented?

The Server and Storage Team has requests to restore data over the Council's server estate on a daily and weekly basis. The verification of SQL Server backups and testing of recovery are standard database administrator processes undertaken within the Council. The same backup and recovery processes are utilised across the SQL Server estate. Requests for database refreshes and data recovery from backups are frequently undertaken and by definition therefore verify the backup and recovery mechanism. As a regular maintenance activity, whenever patching of SQL Server or the associate Backup software (Quest Litespeed) takes place, restores are verified to prove that they are reliable and useable.

Training

Record training undertaken by staff responsible for digital security, storage and backup procedures, Disaster Recovery and Business Continuity in Appendix 2. Keep this log updated as part of the DMS. Is the training adequate for the present needs of the service? What further training is required?

ITC staff are responsible for digital security, storage and backup procedures, Disaster Recovery and Business Continuity. HER staff have undertaken HBSMR System Administration training, internal GIS training, and internal Data Protection and Security Essentials training, which includes GDPR and must be refreshed annually.

Responsibilities

Who is responsible for keeping this Data Management Statement up to date?

Name:

Job title:

Email:

Telephone:

Who is responsible for data backups?

<u>Database</u>

Name: xxx

Job title: Systems Integration Officer

Other servers

Name: xxxxt

Job title: ICT Server, Storage & Print Manager

Who is responsible for testing data recovery?

Database

Name: xxxx

Job title: Systems Integration Officer

Other servers

Name: xxx

Job title: ICT Server, Storage & Print Manager

Who is responsible for Disaster Recovery and Business Continuity?

Disaster Recovery

Name: xxx

Job title: ICT Operations Manager

Business Continuity

Name: xxxx

Job title: Service Manager (Joint Emergency Planning Unit)

xxxx Council acknowledges the principles and best practice contained in the National Security Code of Practice, including provision for exceptional decisions to deposit a security copy with another heritage organisation for safeguarding, as set out in the Code's Access Protocol.

Signed for and behalf of xxxx Council

By*: xxxxx

Signature: …………………….

Title: Senior Archaeologist
Email:xxxx
Telephone: xxxx

*We recommend the signatory is part of the HER senior management team.

Part B

Data security

Please describe how anti-virus and firewall protection is managed, and how access and passwords are controlled. Who is responsible for data security? Are these procedures adequately documented?

The IT team carefully manages the Council's anti-virus measures, firewalls and a number of other security mechanisms. They also have strict access controls and password policies in place. The Council is independently audited each year on these measures (and lots of others) as part of its annual Public Shared Network (PSN) accreditation and currently has a PSN certificate of compliance, which will expire in August 2021.

Physical storage

Give a brief description of where paper-based sources are held, explaining if these are held in the office, in basement storage, off-site storage or commercial storage. Is the storage secure? Who has access?

The Archaeology Service's grey literature reports, aerial photographs, printed site photographs, journal offprints, library books, microfiche, hard copy maps, very small collection of Ordnance Survey record cards and supplementary Monument files are all stored in lockable cupboards on the first floor of the xxxx office. The office is only accessible to those with a xxxx Council pass and no documents are taken outside of this office by members of the public. A small quantity of the older grey literature reports may be the only existing copies, but following a disaster situation everything else would be replaceable. No primary archive is held by the Archaeology Service. In anticipation of a move into a different service area within the Council in January 2021, plans are being drawn up for the transfer of library books to lockable cupboards in xxxx library.

Give details whether these have been digitised, including any backup and storage arrangements for the digitised copies.

A project to digitise grey literature is currently underway, initially in-house and now with the help of the xxxx. The storage arrangements and back-up procedures for digitised and born-digital files is the same as detailed above. xxxx files are sent via a xxxx secure large file transfer service. Once all hard copy resources (other than library books and offprints) have been digitised, they will be archived or disposed of as appropriate.

Questions to consider:
Have you deposited paper-based sources (record cards, maps, reports, photographs) in a local record office or museum?
Has each component been assessed to decide on the length of retention?

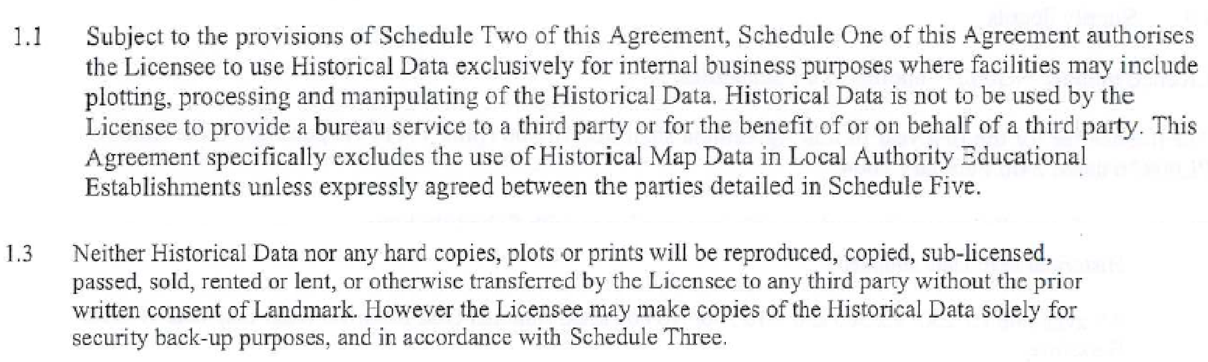
Legal compliance

Describe how you manage compliance with GDPR and any other legal issues in your data.

The Archaeology Service's Data Protection Privacy Notice is available online here: xx As outlined in the HER's Policies and Plans document (sections 4 and 5.2.8), the HER will record on its database those People and Organisations with a direct involvement with the Archaeology Service and the investigation or management of the historic environment of the district in compliance with data protection legislation. Only limited personal data is recorded for living persons, unless they are operating in a professional work capacity and their personal data is already publically available, and for deceased people who have had an important role in xxx historic environment (eg past museum curators or archaeologists). The People record includes the dates of their lifespan with a short summary of their activities and roles.

Portable Antiquities Scheme data is not imported into the HER and not provided to third parties.

PDF maps containing Ordnance Survey base mapping are produced under xxx licence (number xxx), but may not be reproduced by a third party unless they also have their own OS licence. Historical Ordnance Survey maps are similarly licensed to xxx by the Landmark Information Group. They are not covered by our other Ordnance Survey licence and as such are not available to be shared with third parties, even if they have their own OS licence. Here are extracts of our Landmark Licence Agreement:



1.1 Subject to the provisions of Schedule Two of this Agreement, Schedule One of this Agreement authorises the Licensee to use Historical Data exclusively for internal business purposes where facilities may include plotting, processing and manipulating of the Historical Data. Historical Data is not to be used by the Licensee to provide a bureau service to a third party or for the benefit of or on behalf of a third party. This Agreement specifically excludes the use of Historical Map Data in Local Authority Educational Establishments unless expressly agreed between the parties detailed in Schedule Five.

1.3 Neither Historical Data nor any hard copies, plots or prints will be reproduced, copied, sub-licensed, passed, sold, rented or lent, or otherwise transferred by the Licensee to any third party without the prior written consent of Landmark. However the Licensee may make copies of the Historical Data solely for security back-up purposes, and in accordance with Schedule Three.

Questions to consider:

- State whether you have received any advice on GDPR in the data that you collect, whether there are any restrictions on the reuse of third-party data
- Consider whether any permissions need to be obtained to enable reuse of the datasets for the national security copy, or to enable sharing with relevant organisations.

Preservation

Identify and briefly describe data that must be retained to provide HER services and for legal or regulatory reasons, e.g. under an SLA with a neighbouring authority.

- The HER database and GIS
- Linked digital files

- Stand-alone digital files (including policies and procedures, HER access terms and conditions, recording manual)
- Hard copy resources (including the Archaeology Service's library, and grey literature and supplementary Monument files not added to the HER yet)
- Hard copy aerial photographs that are the copyright of others (for example Historic England)
- Data licences with utilities companies, such as xxx

All physical files that have not yet been entered onto the HER database and/or have not yet been appropriately digitised should be retained until such time as it is possible to do this. This includes some grey literature not otherwise held on the ADS and supplementary Monument files. Time will be needed to sort through it and decide what needs to be kept.

We do not have any Service Level Agreements with any other local authorities.

Questions to consider:

- How will you decide which data and information sources should be retained and preserved?
- Consider which information sources and other documents are important to support business processes and should be retained. If paper-based sources have been successfully digitised, consider whether the physical material could be deposited in a local record office. What time or effort would be involved in preparing the data?

Please send your completed form, Part A (signed) and Part B, to HIPsTeam@HistoricEngland.org.uk

Appendix 1: Data and file recovery log

Event e.g. recovery test or incident	Date	Description	Result/Action
Recovery test	19/01/2020	SQL> Processed 65176 pages for database 'HBSMR_LIBRARYLINK_xxx	SQL> RESTORE DATABASE successfully processed 65178 pages in 2.020 seconds (252.077 MB/sec).
Recovery test	19/01/2020	SQL> Processed 100280 pages for database 'HBSMR_xx', file 'HBSMR_xxx' on file 1. SQL> Processed 2 pages for database 'HBSMR_xx', file 'HBSMR_xxx_log' on file 1.	SQL> RESTORE DATABASE successfully processed 100282 pages in 2.024 seconds (387.079 MB/sec).

Appendix 2: Training log

Staff name	Date	Training undertaken	Follow-up/Action
Beth Asbury	24/09/2018	Data Protection Awareness (internal)	
Beth Asbury	11/10/2018	Information Security Awareness (internal)	
Beth Asbury	25/02/2019	ArcGIS (internal)	
Beth Asbury	03/04/2019	HBSMR System Administration (Exegesis) (two days)	
Beth Asbury	27/02/2020	Exegesis webinar on HBSMR	
Beth Asbury	28/05/2020	Historic England webinar on the NRHE to HERs project	
Beth Asbury	10/06/2020	Data Protection and Security Essentials (internal)	Refresher training due by 10/06/2021
Beth Asbury	04/09/2020	Exegesis webinar on LibraryLink	
Beth Asbury	22/10/2020	Historic England webinar on the NSC Protocol and DMS	