[xxxx] Historic Environment Record

Data Management Statement (DMS)

Author(s):	
Origination Date:	28/02/2020
Reviser(s):	-
Date of last revision:	-
Version:	1
Status:	Draft
Summary of changes:	
File name/location:	

Related policies:	Date of last revision	Revision required	Location
Systems Security Policy	November 2019	November 2021	Intranet
Recording Policy	January 2020	January2021	Archives and Heritage
Disposals Policy	January 2020	January 2021	Sharepoint site
Disaster Recovery Plan	March 2018	March 2021	
Index to Reference Collection	January 2020	January 2021	
Recording Manual	March 2020	March 2021	
Prioritised list of backlog	March 2020	March 2021	

Contact HIPsTeam@HistoricEngland.org.uk if you have any queries when completing this form.

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

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 Part1).
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.

Part A (Please complete this section in full).

The HER system and software

The HER includes textual data in a computerised database using HBSMR V5.05, which is linked to spatial data in digital form on a Geographic Information System (GIS) using QGIS 2.14.22

The HBSMR software is an off-the shelf package developed and supplied under licence by exegesis. The database is exegesis hosted and is stored on their London servers.

The GIS layer is a corporate GIS layer with Ordnance Survey data supplied under licence (No 10019331).

Programme components are installed on HBSMR servers and remotely accessed.

The HBSMR system stores data in a SQL Server database, and uses Access for the user interface.

General ICT support is provided by [xxx] and can be contacted on [Tel. number] Option 1. Specialist support for the software is provided by exegesis and can be contacted on [Tel. No] or hbsmr@esdm.co.uk.

A database model (e.g. entity relationship diagram) is stored on [xxx] Sharepoint at Environment and Planning/Archives and Heritage/HER Working Documents/Data Model

Supporting documentation including details of any codes, abbreviations and terminology utilised in the database and GIS is stored on the Archives and Heritage Sharepoint site (at Environment and Planning/Archives and Heritage/HER Working Documents/Recording Manual).

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 database	c 420mb	Exegesis server	Yes
GIS Layer	QGIS Shapefile and mapinfo tab files	C 420mb	Exegesis server	Yes
Stand-alone digital files*	csv, xls, PDF, tiff, jpeg, Microsoft Word,	Sharepoint Library -3451 individual items. Archived H Drive-66GB	HLC, NMP and EUS online at ADS. Other archives stored on CD and archived H drive. All working files stored on archived H drive. Digital library (grey literature and some supplementary files) stored on Sharepoint	Partial
Paper-based information sources	Supplementary files, aerial photographs, building photographs, slides collection, OS cards, grey literature, copies of historic maps		All physical collections are stored at the Records Office in the Classroom, Search Room, Index Room, Repositories and Bunker	Partial

Digital data backup

Back up procedures:

The Exegesis applications are installed on a dedicated virtual machine with SQL databases held on a shared database server. Both are hosted in London in a Tier 1 Virtus datacentre. This includes appropriate physical protection of at rest data, the use of commercially available security software and SSL encrypted data in transit.

There are two different types of backups for hosted clients, on-site and off-site.

On-site

The entire virtual machine is backed up nightly using BackupChain. This is an operational backup for quick recovery of the entire VM in the event of disaster or data loss. The data is stored on an NAS (Network Accessible Storage) device or separate physical server and has a minimum 5 day retention.

Off-site

All critical application components are backed up nightly off-site. This includes the HBSMR and other SQL databases, the HBSMR application folder and other critical files agreed with the HER Officer. The SQL databases have a 30 version retention, other files have a 10 version retention. These may

include other data files held on the hosted server such as documents and images which are not held elsewhere. The data is stored in the cloud using iBackup and protected by client-side encryption with a private encryption key that is not shared with the storage provider.

Training

The HER staff have undertaken HBSMR Administrator training and all other users of the software have completed User training. Basic QGIS training has also been undertaken. All staff have to undertake regular training modules as part of their employment including Information Management and Data Protection Awareness and GDPR Training.

Responsibilities

Who is responsible for keeping this statement up to date?

Name:
Job title:

Who is responsible for data backups?

Name: Exegesis
Job title:

Who is responsible for testing data recovery?

Name:Exegesis
Job title:

[Name of Council/host] 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 [*Local Authority*]

By*: ……..

Signature: ……

Title: ……..

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

Part B (Please either complete this section in full, or provide references and links to where information is held within existing policy documentation).

Data Security

Access to HBSMR is password configured by user, in order that relevant permissions are applied (editing and viewing rights). HBSMR data is protected by an enterprise grade, centrally managed, agent based Antivirus solution which updates its virus definitions daily, has on-access scanning and weekly full scans for non-accessed files. Two enterprise grade virtual firewall appliances in a high availability cluster are run. These appliances are kept up to date with their definitions as soon as new firmware is available The appliances features Intrusion Prevention with regular updates to the patterns. Reviews of the firewall and various security checks are made regularly to ensure integrity and security of the data being protected. More details of both the Antivirus and Firewall solutions can be supplied on request (to Exegesis).
[xxx] network logins are required for HER digital collections stored in the archived H drive and mapped files stored on the P drive. Access to documents on Sharepoint is restricted by the Site Owners (xxx) to named individuals.
Annual mandatory training regarding data management, GDPR and security is undertaken by all staff.
Anti-Virus software and firewall technology is in use across the council network. For further information contact (xxx), Information Governance Officer.

Physical Storage

All physical data associated with the HER are stored within the [xxx].
Grey literature and general reference material is located within the public search and index rooms, in an area protected by a security door. No documents are taken beyond this door by members of the public. The majority of the grey literature, where not already accessible on ADS/OASIS, has been digitised and is accessible on Sharepoint. This is a continuing project.
Aerial photographs, where taken for archaeological purposes, maps, outsize documents and the few small archives the HER is storing until the ARC is ready to accept are kept in the archive's repositories. The HER collection of slides, Supplementary Files, OS Record cards, Buildings Photographs and county-wide vertical aerial photograph collections are held in the Classroom, which is a locked room accessible only by staff. The supplementary files have been digitised. Some have been added to Sharepoint. Documents are added on an ad hoc basis, but not all will be required as many are photocopies of sources which are already held elsewhere. There are also

GDPR issues with some of the documents and each must be assessed by the HER Advisor prior to production.

Project archive data is kept either in the Classroom or in the staff office. Most of the county-wide projects have been entered onto the database and are available digitally (EUS, NMP, HLC available online;
No plans for the retention or otherwise of the data have yet been formulated, although it is anticipated that at some future stage the material comprising this collection may be digitised and fully accessible (ideally through the computerised HER itself). Whilst acknowledging this as a desirable goal the HER will, however, retain a reference collection until such time as its relevant content has been processed into the HER database (or is digitally available elsewhere) and all paper and hard copy material has been appropriately archived (whether at the [xxx].
.

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

[xxx]as part of the wider [xxx], has been guided by [xxx] policy with regards to GDPR. Guidance on copyright issues is drawn from the Records Office.
Customer enquiries are recorded on a Sharepoint database. Access is only allowed to users approved by the Archives and Heritage managers. The minimum personal data necessary is recorded for business purposes. No details are forwarded to other third party organisations. At present, we do not contact the enquirer other than for the purposes of the enquiry and the data is only used for the compilation of usage statistics. All enquiry data is deleted after two years.
No personal data is now recorded within the HER database. In the past, some personal details were recorded (mostly personal names) and every attempt has been made to ensure that these have now been removed. Some personal names may still exist on the database and in the rare cases personal data is identified on the HER it is removed immediately.
Some of the HERs supplementary files, which exist as paper and digital records, include personal data and it is the responsibility of the HER Adviser to act as a 'Gatekeeper' and ensure that any such information is redacted prior to third parties viewing the files or, if required, restricting access entirely.
No extra permissions are considered necessary for reuse of the key HER datasets for the national security copy.

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

SLA with subscribing authorities states that the HER database and related data should be made accessible, although no specifics are provided in relation to the 'related data'.

All business critical data is held on the remote servers; this is the data that is essential in providing essential HE information to key stakeholders.

Major project archives, including the EUS, HLC and NMP surveys, have already been archived on ADS.

All physical data that has not yet been entered onto the HER database and/or has not yet been appropriately digitised (to accepted archive standards) should be retained until such time as it is possible to do this. This includes some grey literature not otherwise held on ADS and archive project data.

The aerial photograph collection has been deposited with the National Monuments Record; some has been digitised (and available on ADS), but ideally the entire collection should be available online. The HER also holds a significant number of aerial photographs of which it does not hold the copyright. Most of these have also been archived at the National Monuments Record by the Copyright holder.

Much of the physical data has been entered onto the HER database, but in some cases enhancement of the data is required; this includes OS Record Cards, Supplementary Files, NDC SMR Records. Ideally, this data should be digitised as a priority.

The HER currently holds a significant amount of reference material that is considered to be an asset to the service for reference purposes, but which is not strictly necessary to support ongoing business processes. This includes the general library and national journals.

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