[redacted] Historic Environment Record

Data Management Statement (DMS)

Author(s):	[redacted]		
Origination Date:	24th April 2020		
Reviser(s):			
Date of last revision:			
Version:	1		
Status:	Live		
Summary of changes:			
File name/location:			
Related policies:	Date of last revision	Revision required	Location
Systems Security Policy	April 2020	April 2021	[redacted]
Recording Policy	April 2020	April 2021	[redacted]
Disposals Policy	April 2020	April 2021	[redacted]
Disaster Recovery Plan	April 2020	April 2021	[redacted]
Index to Reference Collection	2019	2020	[redacted]
Recording Manual	2019	2020	[redacted]
Prioritised list of backlog	2019	2020	[redacted]

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 a customised Access 2010 & SQL database: Historic Buildings, Sites and Monuments Records (HBSMR V 5) which is linked to spatial data in digital form on a Geographic Information System (GIS) using ArcGIS 10.5.1.

The HBSMR software is customised off-the shelf package developed and supplied [under licence] by Exegesis SDM.

The database is stored on the corporate network at the following location: Front End: [redacted] *SQL Server: SERVER=WCC-SQLDBP-04\SQL002;DATABASE=HBSMRv5.*
The GIS layer is stored on corporate network at the following location [redacted] *and is not part of a corporate GIS.*

Programme components are installed on a Remote Desktop Sever and accessed via [redacted]*.The HBSMR system stores data in a SQL Server database, and uses Access for the user interface.*

General ICT support is provided by [redacted] *and can be contacted on* [redacted] [redacted] *Specialist support for the software is provided by Exegesis and can be contacted on* [redacted]

Supporting documentation including details of any codes, abbreviations and terminology utilised in the database and GIS is stored within [redacted]

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	HBSMR: Access Front End And SQL Server Tables: SQL Server 2014 SP3	38.4mb 1.6gb (HBSMRv5) 3.7gb (HBSMRGateway) 256mb (HBSMR Library Link)	[redacted] *SERVER=WCC-SQLDBP-4\SQL002;DATABASE=HBSMRv5*	Yes - Within HBSMR Audit Trail
GIS Layer	Spatial data is fully integrated into HBSMR tables	As above	[redacted] *SERVER=WCC-SQLDBP-4\SQL002;DATABASE=HBSMRv5*	Yes – Within HBSMR Geographic Position Metadata
Linked digital files	PDF, TIFFS	44.8GB Tiff Backups: 572GB	[redacted]V:) V:\HER_System	Yes - HBSMR Source Record, Audit Trail and within Document Properties
Stand-alone digital files*	JPG, TIFFS of Aerial Photographs	3.1 GB Tiff Backups: 89.7GB	[redacted] V:\HER_System	Yes – Document Properties
Paper-based information sources	Paper Reports, Aerial Photos, Map Transcriptions, Refence Collection	68 filing cabinet drawers (17 filing cabinets – approx. 9500 records) 2 map cabinets (250 maps) 28 box files of newsletters/transactions,300+ transactions/ books, 3000 Aerial Photographs.	HER Office and Public Desk Area	Yes – HBSMR Source Record, Audit Trail and HER Reference Collection List

*For example, may include NMP, HLC, UAD, EUS data not integrated into the HER system.
** 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; https://www.ukdataservice.ac.uk/manage-data/document/metadata.aspx and https://www.agi.org.uk/agi-groups/standards-committee/uk-gemini

Digital data backup

Back up procedures:

SQL Platform Backup Policy

Frequency

Full Backup – Weekly, Sundays
Differential – Mon-Sat Night
Logs – Hourly, Business Hours, Mon-Fri

Procedures

Current – NetBackup 8.2 SQL Agent writing to HP Storeonce, retention periods: Full 1 Month, Diff 2 Weeks, Log 2 Weeks

New (Live this week, 20/04/2020) – NetBackup 8.2 SQL Agent writing to local NexSAN, followed by duplication to offsite* NexSAN, retention periods: Full 1 Year, Diff 1 Month, Log 2 Weeks

Testing

HER is not specifically tested, however we regularly carry out ad-hoc restores for the same or identical backup policies.

Hyper-V Backup Policy – (RDS)

Frequency

Full Backup – Weekly, Sat/Sun
Differential – Mon-Fri Night

Procedures

Current – NetBackup 8.2 Hyper-V Agent (VSS Snapshot) writing to HP Storeonce, retention periods: Full 1 Year, Diff 1 Month

New (Live this week, 20/04/2020) – NetBackup 8.2 Hyper-V Agent (VSS Snapshot) writing to local NexSAN, followed by duplication to offsite* NexSAN, retention periods: Full 1 Year, Diff 1 Month

Testing

HER is not specifically tested, however we regularly carry out ad-hoc restores for the same or identical backup policies.

File Server Backup Policy – (All file stores)

Frequency

Full Backup – Weekly, Sat/Sun
Differential – Mon-Fri Night

Procedures

Current – NetBackup 8.2 Windows File Server Agent writing to HP Storeonce, retention periods: Full 1 Year, Diff 1 Month

New (Live this week, 20/04/2020) – NetBackup 8.2 Windows File Server Agent writing to local NexSAN, followed by duplication to offsite* NexSAN, retention periods: Full 1 Year, Diff 1 Month

Testing

HER is not specifically tested, however we regularly carry out ad-hoc restores for the same or identical backup policies.

** Note the offsite NexSAN is [redacted] in a separate building, however we have plans to move this to another site [redacted] once initial seeding is complete.*

Testing back up procedures:

HER is not specifically tested, however we regularly carry out ad-hoc restores for the same or identical backup policies.

Testing of backups will be integrated into the forthcoming IT business continuity plan.

Training

All storage, backup, restores and testing procedures are undertaken by fully qualified ICT Hard DBA Engineers (where not automatic).

Historic Environment Record Team members have undertaken training in HBSMR Administration including tasks such as backup and maintenance, provided by Exegesis SDM. Staff have also undertaken elearning on cyber security including data protection & GDPR as well as corporate induction into IT systems undertaken on joining the County Council.

Responsibilities

Who is responsible for keeping this statement up to date?

Name: [redacted]
Job title: Historic Environment Record A[redacted]

Who is responsible for data backups?

Name: [redacted]
[redacted] [redacted]

Who is responsible for testing data recovery?

N/A – backup testing forthcoming. Currently only performed by adhoc restoration of databases on the same server performed by Hard DBA Engineer.

[redacted]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*: ..[redacted]

Signature: ......[redacted]..................

Title: ...Historic Environment [redacted]

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

Please describe how anti-virus and firewall protection is managed, and how access is controlled.

WCC IT Access Control Policy: [redacted]
WCC IT Anti-virus Policy: [redacted]
WCC IT Firewall Management: [redacted]

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. Give details whether these have been digitised.

All paper original sources are stored in locked filing cabinets [redacted] Many of the sources are digitised. Other reference sources are also stored at this location (In locked glass fronted cabinet and 2 Map cabinets) and within the main HER Office on shelves beside staff desks.

No records are deposited in archives or museum and retention lengths are considered for all items.

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? Yes

Legal Compliance

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

GDPR Compliance policy: [redacted]
Copyright Agreements: [redacted]

Advice from County Council GDPR Team has been taken and all staff have undergone GDPR Training.

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.

HER Database and GIS
Digital Sources (SWR Sources saved on (V:))
Paper Sources (Stored within filing cabinets at HER Desk)
Hard Copy Aerial Photographs (Stored in Glass Cabinet at HER Desk)

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