Heritage Information Access Strategy

National Security Copy:

Field Test

Historic England

Document Control Grid

Project Name:	HIAS National Security Copy: Field Test
Historic England Reference Number	8077
Organisation	Association of Local Government Archaeologists (ALGAO) UK
Author:	Ben Wallace (Chair ALGAO (UK): Historic Environment Record Committee) benwallace@warwickshire.gov.uk 01926 412735
Origination Date:	08 May 2021
Reviser(s):	
Date of last revision:	02 June 2023
Version:	v. 3.0
Status	Final Document
Summary of Changes	
Circulation:	Project Team, Historic England
Required Action:	Publication and Archive
File Name/Location:	8077 Project Report.docx
Approval:	Not required

Contents

1. Introduction

This report details the results of the HIAS National Security Copy Field Testing Project which took place between January – May 2021.

Background to project

The Heritage Information Access Strategy (HIAS) is a programme of interlinked projects designed to simplify and improve public access to heritage data held or generated by Historic England, by Local Authority Historic Environment Records (HERs) and by other bodies. Central to HIAS are eight principles, including: "Historic England should, on behalf of the nation, ensure that a security copy of all such data exists" and "such data or knowledge should not be at risk of loss, fragmentation, inundation (in data), or system obsolescence".

The National Security Copy (NSC) standard establishes trust in the long term preservation and access of historic environment records created and held by HIAS partners. In the event that these records become at risk, a code of practice can be activated to safeguard the NSC.

This project sought to test how the arrangements set out in the NSC Code of Practice work in real-life conditions and to determine the likely implications and costs involved if the Access Protocol within the Code of Practice is invoked.

This project contributes to Historic England's strategic activity "expanding the digital availability of our assets to improve both access to our resources and users' experience of them", identified in the current Corporate Plan 2019-22, the Corporate Plan 2020-23 and in Historic England's commitment under the Culture White Paper (2015) to work with local authorities to enhance and rationalise national and local heritage records over the next ten years so that communities and developers have easy access to Historic Environment Records.

This project is central to the delivery of the Heritage Information Access Strategy (HIAS). HIAS is a partnership programme led by Historic England on behalf of the sector, which aims to improve and simplify access to heritage data to support the planning process and for use by local communities. At the heart of the strategy is the role of Local Authority Historic Environment Records (HERs) as the first point of call and primary trusted source of information about the historic environment (HIAS Principle 1).

Consultants were engaged by Historic England to develop best practice for the NSC and to set out how, through an Access Protocol, access to and transfer of HER resources to a third party could be achieved to ensure security and integrity of data should a trigger event occur. The Access Protocol forms part of Historic England's funding contract with Local Authorities when HERs take part in the Data Supply and Reconciliation project to integrate the terrestrial portion of the National Record of the Historic Environment (NRHE) into their databases. The Protocol states that: "the instances in which an organisation may need to safeguard its dataset by depositing a security copy with an external body include:

- Technical concerns over the stability of the IT system or infrastructure; and/or
- Financial/resourcing concerns over the sustainability of the service".

One of the recommendations in the consultant's report into how the NSC Code of Practice is to be implemented was that this transfer mechanism should be tested.

Aims and Objectives

The main aim of this project was to test how the implementation of the NSC Access Protocol can be achieved in a number of real life scenarios.

This included ensuring that the data held as part of the HIAS National Security Copy could (when at risk) be:

- taken from one HER utilising their digital backups,
- testing a series of scenarios covering different HER systems including a bespoke HER,
- securely held by a third party until measures were taken to mitigate the risk,
- be transferred, if necessary, to another HER database to re-establish a service irrespective of the host systems used by the two HERs.

Further this project explored:

- What documentation and metadata is required from the original HER to facilitate the transfer. Specifically, whether the Data Management Statements (DMS) completed by HERs are adequate for this purpose and if not what additional metadata or information is required
- What the required steps are, should this need to be carried out in a real scenario
- What the outline costs might be in carrying out the procedure in real life
- What arrangements are needed for the safeguarding of stand-alone digital files and paper-based information sources that allow re-instatement of the full HER service

The NSC Code of Practice applies to all organisations participating in HIAS, however this project was designed to test the process as it relates to HERs only. It took into account the range of situations encountered by the 83 HERs in England and also the varying software platforms used by HERs (including bespoke systems).

Project Team:

- Quinton Carroll, ALGAO (Project Executive)
- Ben Wallace, ALGAO, (Project Manager, also representing Warwickshire and Solihull HERs)
- Chris Webster, South West Heritage Trust (representing Somerset and Bath and North East Somerset HERs)
- Andie Webly, Worcestershire County Council (representing Worcestershire HER)
- Catherine Dove, Exmoor National Park (representing Exmoor HER)
- Tim Grubb, Gloucestershire County Council, (representing Gloucestershire HER)
- Andy Jones, Historic England (Arches database expertise)
- Crispin Flower, Exegesis Spatial Data Management (HBSMR technical specialist)
- Tim Evens, Archaeology Data Service (third party data holder)
- Martin Newman, Historic England (NSC process owner)
- Jane Golding, Historic England (Heritage Information Partnerships (HIPs) team)
- Jenni Butterworth, Drakon Heritage and Conservation (Project Assurance Officer)

2. Methodology

The objective of this project was to test the main elements of the National Security Copy Code of Practice.

The National Security Copy standard has been developed to establish trust in the long term preservation and access of historic environment records created and held by local authorities. In the event that these records become at risk, a code of practice can be activated to safeguard the NSC. The Code of Practice covers two types of security copying to safeguard data maintained as the National Security Copy:

NSC1: Consistent routine backups where security copies are made of a heritage dataset by an organisation – covered by the NSC Data Management Statement (DMS): https://historicengland.org.uk/content/docs/her/data-management-statement/).

NSC2: Exceptional decisions to deposit a security copy with another heritage organisation for safeguard – covered by the Access Protocol: https://historicengland.org.uk/content/docs/her/national-security-copy-accessprotocol/

Method to test NSC1

When the Access Protocol is invoked the DMS forms essential documentation to accompany the data being safeguarded. This project tested the efficiency of the NSC DMS including the scenario where a DMS does not exist.

Data was gathered from available HER survey responses and HER audits to determine the current rate and trend of secure backups of HER data being made and the number of DMSs that are currently available.

Members of the project team were questioned over their particular circumstances regarding secure backup of HER data and having a DMS and, where available, a copy of each DMS from each HER was obtained.

Recommendations for the revision of the DMS template is detailed below as a result of detailed testing from this project including feedback from the project team and a detailed review of the DMS itself.

Method to test NSC2

NSC2 is currently broken down into four stages of implementation, which are detailed as:

> ***Stage 1: Assessment of risk in response to a trigger event.***
>
> *Technical concerns over the HER IT system or infrastructure, and/or financial/resourcing concerns over the sustainability of the HER service may arise and this may spur a trigger event such as:*
>
> - *Concerns that an existing database is unstable and is being moved to a new system.*
> - *Reduction in staff and/or expertise to a level where the organisation can no longer ensure that neither best practice is being followed, nor responsibility is maintained for the security of the data and of the HER's essential documentation and information sources.*
>
> *When a trigger event occurs:*

- *The HER informs Historic England of the situation (or Historic England is notified by other means).*
- *Historic England assesses the risks and supports the local authority in management of the situation (the DMS requires details of a non-HER contact for this purpose, in addition to the HER contact).*

The assessment by Historic England reveals either:

- *Risk to security of the data is low– the situation can be managed in-house by adhering to best practice as set out in the HER's Data Management Statement. Historic England will continue to monitor the situation.*
- *Risk to security of the data is high – this is most likely under a trigger event where no adequate levels of staff and/or expertise are in place to ensure that DMS best practice is being followed and responsibility is maintained. The process then moves to stage 2.*

Stage 2: Stakeholder consultation

Following consultation and with stakeholder agreement, Historic England initiates implementation of the Access Protocol. Once the Protocol has been invoked, Historic England oversees the process, negotiates permissions, and commissions a third-party service to manage the technical stages of the transfer.

Stage 3: NSC preparation and transfer

Preparation of a security copy of the data, along with supporting documentation and resources (policy documentation in particular, including the DMS and index to the HER's reference collection) to be transferred.

Transfer of the security copy and supporting resources to a temporary safeguard. On-going storage and security maintenance of the data by the intermediary host.

The DMS identifies stand-alone digital files and paper-based information sources that allow re-instatement of the full HER service. Although the NSC Access Protocol does not include transfer of these components to a third party with the data for temporary safeguard, the process should ensure that arrangements have been put in place to guarantee their continued security and survival.

Stage 4: Reinstate the data and re-establish service

The NSC is a copy of HER data held as security against loss or corruption during a trigger event. In the majority of circumstances it should be possible to delete the security copy on successful completion and testing of:

- *Either re-instatement of the database and service by the local authority,*
- *Or transfer of the data and service to a neighbouring HER without recourse to the security copy.*

However, exceptional circumstances may require the security copy itself to be transferred to a new host.

This project tested all elements of these four stages amongst a range of scenarios determined by a combination of the type of HER software used and the circumstances of the HER host or service organisation.

This included the following HER Software:

- HBSMR (approx. 76% usage amongst HERs)
- Bespoke HER Software (approx. 18% of HERs)
- HEROS (approx. 3% of HERs)
- Arches (approx. 1% of HERs)

The following host or service type:

- Unitary/District/Borough Council (approx. 50% of HERs)
- County Council (approx. 33% of HERs)
- National Park (approx. 7% of HERs)
- Trust (approx. 3% of HERs)

It was not feasible to test ever single combination of HER software and host/service organisation as part of this project but the following combinations were used which covered a range of distinct circumstances believed to be sufficient to adequately test the NSC Access Protocol.

Scenario 1: Unitary HBSMR HER (Solihull) to County HBSMR HER (Worcestershire)

Scenario 2: County Bespoke HER (Gloucestershire) to County HBSMR HER (Warwickshire)

Scenario 3: Trust managed HEROS HER (BaNES) to National Park HBSMR HER (Exmoor)

Scenario 4: National Park HBSMR - remotely hosted (Exmoor) to County HER (Warwickshire)

Scenario 5: Arches Database (Historic England) to County HBSMR HER (Warwickshire)

Other scenarios were considered as part of the project, however rather than being tested in full these were discussed amongst the Project Team to consider the hypothetical feasibility of these scenarios and any issues that could arise.

Testing of NSC2 Stage 1 (assessment of risk in response to a trigger event) was carried out by looking at the different scenarios, considering the different trigger events that can occur and exploring the type of assessment process that will be used by Historic England to determine if an HER is determined at sufficient risk or not.

To test NSC2 Stages 2 to 4 a Test Script (Appendix 1) was used for each scenario. This consisted of the following key steps:

1. **Stakeholder consultation**
2. **Initiate access protocol**
3. **NSC preparation for transfer**
4. **Data transfer**
5. **Check if data transfer is successful**
6. **Reinstate the HER**
7. **Deletion of security copy of HER data**

The use of a Test Script for each scenario allowed a consistent framework where each step could be documented to help inform analysis and discussion later on in the project.

Other digital files and physical sources held by HERs

For each HER the DMS should identify stand-alone digital files and paper-based information sources to allow re-instatement of the full HER service. The NSC Access Protocol does not include transfer of these components to a third party or destination HER and as such it was not included as part of this project for detailed testing. However, consideration was given to these other digital files and physical sources in the analysis and discussion phase of this project in particular to understand what kind of arrangement could be needed to guarantee their continued security and survival and how they could be transferred to a different host.

Consideration of copyright including data rights and security

During testing, different aspects of copyright, including data rights and data security, was considered including licencing, GDPR, access rights, data sharing agreements, data backup and data security.

Review Phase

Once the testing process was complete there was a period of analysis, discussion and review. To help frame this review a series of questions was proposed and the pertinent points and conclusions from this review are included below.

3. Results

Two areas of testing took place, the first was in relation to the National Security Copy 1 phase (NSC1). The second area related to the National Security Copy 2 phase (NSC2) where the data from one HER is extracted and transferred to a different HER.

NSC1 Testing

The NSC1 ensures consistent routine backups and security copies are made of HER data by a host organisation and this process is detailed within the NSC Data Management Statement (DMS).

To understand compliance with NSC1 we looked at data from the 2020 HER Survey which shows that all respondents (79 HERs) considered that backups of their HER and GIS data was made, with almost two thirds also being able to identify who was responsible for these backups. Around 70% claimed daily backups were being made although most were not sure where the backups were stored or how long they were kept for.

On a more negative note only a quarter were able to confirm regular testing of backup and security procedures and again around only a quarter claimed adequate documentation regarding data backup and security.

For a fuller compliance with the NSC1 part of the protocol we looked at how many HERs had a completed DMS and as of March 2021 this was just 24 HERs (30%) although this was increasing in number, mostly due to such initiatives as the HIAS NRHE to HERs Programme and HER Audits.

As part of this project we collected DMS documents from each HER involved in a test scenario and compiled responses from HER officer's experience with completing a DMS. Most of the comments from the Project Team regarding the DMS related to the fact that it was quite complicated and time consuming to complete one and often a fair amount of investigating was needed to uncover all the information and details required for the DMS.

One specific comment from completing the Solihull DMS was that an additional supplementary document detailing all the files and software components needed for running the HER software (HBSMR) was produced and included with the DMS, something that could be a useful addition to the template.

Some discussion has also taken place by HER Officers on the HER Forum regarding the DMS and identified an issue with the need for a database entity relationship diagram. Particularly for HBSMR users this was felt to be superfluous as the model diagram would be the same for all HBSMR users, be complex to source and later understand and ultimately be available if needed from the software provider, Exegesis.

One aspect considered for testing as part of this project was the scenario if an HER enacted the NSC Protocol and did not have a DMS. Exmoor HER did not have a DMS before starting this project and developed one while going through the testing phase of this project. This was useful to test the concept of developing a DMS rapidly with the protocol enacted.

NSC2 Testing

Testing for NSC2 followed the Test Script produced as part of this project (Appendix 1) for each of the five Test Scenarios. A summary of the results can be found in the table below with detailed step by step results per scenario below this.

Scenario No	Origin HER	Destination HER	Data successfully transferred to ADS	Data successfully transferred to Destination HER	HER reinstated	Test considered a success
1	Solihull	Worcestershire	Yes	Yes	Yes	Yes fully
2	Gloucestershire	Warwickshire	Partially	Partially	No	Partial
3	BaNES	Exmoor	Yes	Yes	No	Yes
4	Exmoor	Warwickshire	Yes	Yes	No	Yes
5	Arches (HE)	Warwickshire	Yes	Partially	No	Partial

Scenario 1: Unitary HBSMR HER (Solihull HER) to County HBSMR HER (Worcestershire HER)

Scenario 1 was chosen to test one of the simplest scenarios we could envisage, that is transferring an HER where the Origin HER and Destination HER are using the same HER software and in very similar versions and states, in this case HBSMR from Solihull HER (representing a Unitary HER) to Worcestershire HER (representing a County HER).

Stage 1: Stakeholder Consultation

This is seen as a critical part of the process and involved preliminary dialogue between all parties who were involved when the Access Protocol was initiated. This included:

- Ben Wallace (HER Manager, Warwickshire County Council, who manage the Solihull HER on behalf of Solihull Metropolitan Borough Council) – Origin HER
- Warwickshire County Council ICT Service – Origin HER ICT Service
- Andie Webly (HER Officer, Worcestershire County Council) - Destination HER
- Worcestershire County Council ICT Service – Destination HER ICT Service
- Tim Evans (Deputy Director, Archaeology Data Service) – Intermediary Data Holder
- Crispin Flower (Exegesis) – HBSMR Technical Support

In a real world situation if the Access Protocol had been invoked then the Heritage Information Partnerships (HIPs) Team at Historic England would also have been involved but for the purposes of the testing this was not necessary.

Agreement was reached by all parties as to the process and arrangements for following the Access Protocol before the next stage was started.

Stage 2: Initiate Access Protocol

For the purposes of the test this was initiated by the Project Manager, Ben Wallace. This would normally be carried out by the Historic England HIPs Team.

Ben Wallace started the process on 9th March 2021

Stage 3: NSC Preparation for Transfer

Ben Wallace took copies of all the Solihull HER digital database files including the front end, SQL data (BAK file), spatial data and all supporting documentation including the Data Management Statement (DMS), policy documentation and index to the HER's reference collection. All these files were placed in a folder with as much of the original folder structure intact as possible. A list of all these files and subfolders was produced using the method detailed in the Test Script, this was saved as a Word Document. The folder with all the files (at 654MB in size) was then compressed into a single Zip file 363.4MB in size.

Ben Wallace then emailed Tim Evans at the ADS on 9th March at 1pm to request an FTP site to be able to upload the data to ADS. Ben included the total file size and the Word document detailing the files and folders which would be included in the Zip file.

As part of the preparation an estimation was made of the size of all the other (non database) digital data which formed part of the Solihull HER. This was estimated by Ben Wallace to be around 75GB in size, mostly from the Solihull HER digitised Aerial Photography collection.

Stage 4: Data Transfer to Intermediary Data Holder

Tim Evans emailed Ben Wallace a link to use a FTP site to upload the Zip file at 1:20pm on 9th March. Ben Wallace uploaded the Zip files at 1:30pm on 9th March, the upload took 4-5 mins at 12Mbps (using home broadband). Scanning and checksumming took place on the FTP site at less than 60 seconds.

Stage 5: Check if data transfer is successful

The ADS took the data from the FTP site and loaded it into their servers running tests and checks on the data. Tim Evans emailed Ben Wallace to state the transfer had been successful stating "files received by ADS, checksums created, moved into ingest, moved into a 'dark archive', files retrieved, files verified against checksum (i.e. they match what we were given). Main delay was getting the files off ADS VM into FTP area (network "issues")". At this point the Solihull HER had successfully been transferred as a security copy outside of the host/origin HER.

Stage 6: Reinstate the HER

Tim Evans emailed Andie Webly with details of an FTP site to download the Solihull HER data (as a single Zip file).

Andie then downloaded the data and placed it in an area on Worcestershire County Council's file system which was backed up. At this stage the destination HER would normally send a copy of their DMS (showing they have adequate ICT backup and security processes in place) to Historic England. For the purposes of this test Andie Webly had already emailed a copy of Worcestershire HER's DMS to Ben Wallace fulfilling this part of the test.

Andie Webly then investigated how the Solihull HER could be reinstated to load the database and prove the HER functioned intact as a copy. Unfortunately when Andie asked the Worcestershire ICT Service if they would be able to help with this earlier in the Project (around end of February) they explained that it would be complicated, needing to go through their Digital Transformation Prioritisation Board and would need to ensure availability of someone from their infrastructure team. Consequently, the Worcestershire ICT Service felt they did not have the capacity to be able to help reinstate the Solihull HER to test it as a working HER database.

Exegesis were then contacted to explore other possibilities to reinstate the Solihull HER database. Exegesis suggested that if a full test could not go ahead on Worcestershire's servers then they could use one of the Exegesis remote servers to demonstrate the restoring of the Solihull HER to complete the test. All parties involved were contacted, this was agreed and enacted. The details of the webserver, login and password were supplied to Andie Webly who then logged in and was able to confirm access to the Solihull HER database in full with screenshots provided to the Project Manager as proof of the successful test.

Scenario 1 Result: Full test complete and successful. However, a number of issues were identified particularly by Worcestershire ICT and Data Compliance officers, these are discussed in detail in section 4 (Analysis and Discussion) below.

Scenario 2: County Bespoke HER (Gloucestershire HER) to County HBSMR HER (Warwickshire HER)

Scenario 2 was chosen to test a bespoke software HER which we envisaged would prove difficult to both extract the data and reinstate the HER.

Stage 1: Stakeholder Consultation

This took place before the Access Protocol was initiated and included:

- Tim Grubb (HER Officer, Gloucestershire County Council) – Origin HER
- Ben Wallace (HER Manager, Warwickshire County Council) – Destination HER
- Gloucestershire County Council ICT Service – Destination HER ICT Service
- Warwickshire County Council ICT Service – Destination HER ICT Service
- Tim Evans (Deputy Director, Archaeology Data Service) – Intermediary Data Holder

In a real world situation if the Access Protocol had been invoked then the Heritage Information Partnerships (HIPs) Team at Historic England would also have been involved but for the purposes of the testing this was not necessary.

At this stage (February 2021) Tim Grubb contacted Gloucestershire ICT Service and discovered that unfortunately there was a moratorium on project work until after the new ICT contract started on 1st April. This led to some doubt that Gloucestershire HER could take part in the project but after discussion with the Project Manager, Ben Wallace, it was agreed to pursue what was achievable with minimal or no help from Gloucestershire ICT Service and that this would in effect test a scenario with an HER with an 'unsupportive' ICT Service.

Stage 2: Initiate Access Protocol

For the purposes of the test this was initiated by the Project Manager, Ben Wallace, at the beginning of March 2021. This would normally be carried out by the Historic England HIPs Team.

Stage 3: NSC Preparation for Transfer

After some initial discussions with Gloucestershire ICT Service it was left to Tim Grubb to extract what data he could from the Gloucestershire HER himself.

Tim found that large text description exports into Excel xls exports were problematic in truncating the data leading to data loss.

By 25th March Tim had managed to extract all the data and put together some of the documentation and a file list. The files exported were mostly csv/Excel files of the HER database tables with accompanying glossaries with the remainder made up of large html reports which was the only way he found to export the free text. The files also included copies of all of the digital source work reports and images that were linked to the records.

The total size of all the files was 94GB.

Stage 4: Data Transfer to Intermediary Data Holder

Tim Evans emailed Tim Grubb a link to use a FTP site to upload the files on 26th March.

Tim Grubb attempted to upload the files but needed to create a Zip file of all the files and folders. However, the file was 88GB in size which proved too large for the first FTP site (which had a single file limit of 32GB).

Tim Evans then sent a link to a new FTP site on 30th March with a higher single file size limit. Tim Grubb split the files down to smaller Zip files and removed subdirectories which appeared to be causing a problem in the transfer, however he still struggled to upload all the files with the transfer taking a long time (often overnight) but often failing.

Eventually a suitable number of files was received by the ADS to continue the test.

Stage 5: Check if data transfer is successful

The ADS took the data from the FTP site and loaded it into their servers running test and checks on the data. Not all files were received by the FTP at ADS from the Gloucestershire HER but it was felt after discussion with all parties that it was enough to continue the test.

Stage 6: Reinstate the HER

Tim Evans then sent an FTP link to Ben Wallace at Warwickshire HER on 15th April to download the Gloucestershire HER files.

Ben Wallace then downloaded the data on 16th April and placed it in area on Warwickshire County Council's file system which is backed up. At this stage the destination HER would normally send a copy of their DMS (showing they have adequate ICT backup and security processes in place) to Historic England. For the purposes of this test Warwickshire already have a DMS fulfilling this part of the test.

Ben Wallace verified the files and investigated if there was any way to open them or try reinstating the HER but the lack of completeness of the files, and the fact they were just exports not backup copies to be restored, meant it was decided to end the test at this point.

Scenario 2 Result: Test complete but only partially successful.

Discussion

Tim Grubb had issues sending individual files by FTP and also large ZIP files. Subdirectories of folders needed to be removed and he had to zip individual folders which led to a loss of folder structure and would have meant great difficulties in putting back together the Source and Photo files from the HER

for it to work properly. Tim Evans suggested that there was a possibility the file transfer issues could have been due to the file and folder structures and contents of the zip files but that it could also have been network/internet connectivity issues. It was out of scope of this project to resolve what the file transfer issues were but certainly something to consider whether this is an appropriate method particularly if large files with complex folder structures and sub directories need to be transferred.

The project unfortunately coincided with the changeover of contracts with Gloucestershire County Council's ICT suppliers. In normal circumstances it may have been possible to arrange a copy of the HER backup and supply relatively quickly anything extra needed (e.g. management documentation, source works pdfs and images etc).

In terms of file transfer the same problems with the file transfer service may not have been encountered with an official backup from the HER database. As the latter wouldn't have included source work pdfs or photos, which were the folders which caused the problem and were unable to be transferred.

Tim Grubb also made one other point which was if as an alternative, such as a hard drive or other physical backup solution, was used this may have encountered other issues regarding data protection and data security.

Scenario 3: Trust managed HEROS HER (BaNES HER) to National Park HBSMR HER (Exmoor HER)

Scenario 3 was chosen to test two very differently managed HERs with two distinct HER software.

BaNES HER uses the HEROS software which is open source and typically uses a web browser to provide access to the HER records. One simple way of allowing access to the HER, and in effect complete a transfer of sorts, would be to allow an external user login to the BaNES HER. This it was felt was a too simplistic approach to data transfer and would not allow for issues such as the server no longer being maintained or accessible. If the data needed to be transferred to another server the full data transfer process would need to be followed and so it was decided to carry out the scenario following the test script as fully as possible.

Stage 1: Stakeholder Consultation

This is seen as a critical part of the process and involved preliminary dialogue between all parties who would be involved when the Access Protocol would be initiated. This included:

- Chris Webster (HER Manager, South West Heritage Trust who manage the Bath and North East Somerset (BaNES) HER) – Origin HER
- South West Heritage Trust ICT Service – Origin HER ICT Service
- Catherine Dove (Conservation Advisor (Historic Environment), Exmoor National Park Authority) - Destination HER
- Jon Coole (ICT Manager, Exmoor National Park Authority) – Destination HER ICT Service
- Tim Evans (Deputy Director, Archaeology Data Service) – Intermediary Data Holder
- Crispin Flower (Exegesis) – HBSMR Technical Support

In a real world situation if the Access Protocol had been invoked then the Heritage Information Partnerships (HIPs) Team at Historic England would also have been involved but for the purposes of the testing this was not necessary.

Agreement was reached by all parties as to the process and arrangements for following the Access Protocol before the next stage was started.

Stage 2: Initiate Access Protocol

For the purposes of the test this was initiated by the Project Manager, Ben Wallace. This would normally be carried out by the Historic England HIPs Team.

Ben Wallace started the process on 10th March 2021

Stage 3: NSC Preparation for Transfer

By 15th March Chris Webster had prepared an export of files from the BaNES HER. This consisted of a MySQL data export of HER text and spatial files together with HER documentation totalling 52MB in size zipped into a single file 15MB in size.

In terms of other digital files considered part of the HER, Chris identified a collection of scanned grey literature reports totalling 12.4GB in size. This was considered out of scope of this project and was not included for transfer.

Stage 4: Data Transfer to Intermediary Data Holder

On 15th March Tim Evans emailed a link to Chris to a FTP site and Chris used this to send the zip file to the ADS that same day.

Stage 5: Check if data transfer is successful

The ADS took the data from the FTP site and loaded it into their servers running tests and checks on the data. Tim Evans emailed on 15th March to state the transfer had been successful and that a new FTP would be created for the data to be downloaded by Exmoor HER.

Jon Coole from Exmoor ICT service successfully downloaded and checked the BaNES HER files on 31st March.

Stage 6: Reinstate the HER

Unfortunately, due to Exmoor ICT staffing capacity issues it was not possible to reinstate the BaNES HER fully in terms of setting up a HEROS software front end, loading in the BaNES HER data and checking the record. It was felt it would have theoretically been possible and together with help from Chris Webster and the HEROS developer fully reinstate the BaNES HER, however for this project the test ended at this point.

Scenario 3 Result: Test complete

Scenario 4: National Park HBSMR (remotely hosted) (Exmoor HER) to County HBSMR HER (Warwickshire HER)

Scenario 4 was chosen to test a remotely hosted HER being transferred to one with no remote hosting.

Exmoor HER uses HBSMR software being remotely hosted on an Exegesis managed server. Theoretically it would have been quite trivial to give access to another party to the Exmoor HER, a login could have been set up with full access to the HER database. However, this was felt to be too simplistic an approach

to take in terms of data transfer and would not allow for issues such as the server no longer being maintained or accessible. If the data needed to be transferred to another server the full data transfer process would need to be followed and so it was decided to carry out the scenario following the test script as fully as possible.

Stage 1: Stakeholder Consultation

This is seen as a critical part of the process and involved preliminary dialogue between all parties who would be involved when the Access Protocol would be initiated. This included:

- Catherine Dove (Conservation Advisor (Historic Environment), Exmoor National Park Authority) – Origin HER
- Jon Coole (ICT Manager, Exmoor National Park Authority) – Origin HER ICT Service
- Ben Wallace (HER Manager, Warwickshire County Council) - Destination HER
- Warwickshire County Council ICT Service – Destination HER ICT Service
- Tim Evans (Deputy Director, Archaeology Data Service) – Intermediary Data Holder
- Crispin Flower (Exegesis) – HBSMR Technical Support

In a real world situation if the Access Protocol had been invoked then the Heritage Information Partnerships (HIPs) Team at Historic England would also have been involved but for the purposes of the testing this was not necessary.

Agreement was reached by all parties as to the process and arrangements for following the Access Protocol before the next stage was started.

Stage 2: Initiate Access Protocol

For the purposes of the test this was initiated by the Project Manager, Ben Wallace. This would normally be carried out by the Historic England HIPs Team.

Ben Wallace started the process on 10th March 2021

Stage 3: NSC Preparation for Transfer

Jon Coole from Exmoor ICT Service felt it would be best to carry out a Data Protection Impact Assessment and obtain a formal signed data sharing agreement by all parties involved in the data transfer. This was put together and signed on 1st April by representatives from Warwickshire County Council, The ADS and Exmoor National Park Authority.

In terms of the data transfer itself it was felt the best method was for Exegesis to transfer the data direct by FTP to the ADS as the data was held on a server managed by Exegesis. Crispin did note that in a real world situation Exegesis could transfer the data direct to the destination HER rather than through the ADS and that the Exegesis servers are secure and backed up just like ADS servers. For the purposes of this test scenario it was decided to follow the test script and transfer the data via the ADS.

Crispin produced a single zip file of the Exmoor HER data including SQL backup, front end files and folders, HER documentation (supplied by Catherine onto the Exegesis server).

Stage 4: Data Transfer to Intermediary Data Holder

At the beginning of April Tim Evans emailed a link to Crispin to a FTP site and Crispin used this to send the zip file to the ADS on 4th April.

Stage 5: Check if data transfer is successful

The ADS took the data from the FTP site and loaded it into their servers running tests and checks on the data. Tim Evans emailed to state the transfer had been successful.

Stage 6: Reinstate the HER

Tim emailed an FTP to Ben Wallace to download the Exmoor HER data on 12th April. The data was download by Ben on 13th April and placed on Warwickshire County Council's file system which is backed up. At this stage the destination HER would normally send a copy of their DMS (showing they have adequate ICT backup and security processes in place) to Historic England. For the purposes of this test Warwickshire already have a DMS fulfilling this part of the test.

Ben unzipped the file and all contents was checked and appeared to be complete.

At this stage discussion took place to see if the SQL backup file of the Exmoor HER could be restored on Warwickshire County Council servers, however it was discovered that unfortunately the SQL server version used by Warwickshire County Council (SQL Server 2014) was inferior to that used by Exmoor HER (SQL Server 2019) and there was no way to export a backup of an earlier SQL version of the Exmoor HER data nor for Warwickshire to use a newer version of SQL server. It was decided at this point to end the test.

Scenario 4 Result: Test complete

Scenario 5: Arches Database to County HBSMR HER

Scenario 5 was chosen to test an Arches database being transferred to another HER. Arches as an HER software is relatively new and with so few HERs using it fully it was decided that Historic England's own internal database using the Arches platform would be perfect to test this scenario.

Stage 1: Stakeholder Consultation

This is seen as a critical part of the process and involved preliminary dialogue between all parties who would be involved when the Access Protocol would be initiated. This included:

- Andrew (Andy) Jones (Developer Team Leader, IMT, Historic England) – Origin Database
- Historic England IMT Service – Origin Database ICT Service
- Ben Wallace (HER Manager, Warwickshire County Council) - Destination HER
- Warwickshire County Council ICT Service – Destination HER ICT Service
- Tim Evans (Deputy Director, Archaeology Data Service) – Intermediary Data Holder

In a real world situation if the Access Protocol had been invoked then the Heritage Information Partnerships (HIPs) Team at Historic England would also have been involved but for the purposes of the testing this was not necessary.

Agreement was reached by all parties as to the process and arrangements for following the Access Protocol before the next stage was started.

Stage 2: Initiate Access Protocol

For the purposes of the test this was initiated by the Project Manager, Ben Wallace. This would normally be carried out by the Historic England HIPs Team.

Ben Wallace started the process on 11th March 2021

Stage 3: NSC Preparation for Transfer

Andy Jones obtained permission to transfer the data from the Historic England Information Management team on 26th March. This allayed any concerns regarding data security and GDPR.

Andy ran an export from the Arches database with the whole process of extracting the components and compiling them ready to send taking around 1hr:

- PGSQL backup – 3mins
- Elasticsearch index dump – 29 mins
- Source code extract – 11 mins
- Documentation extract – 4 mins
- Transfer times in prep for FTP took about 15 mins.

Three groups of data were produced in the following zip files:

- PGSQL dump file (WardenBackUp_v2_20_04_2021.backup - 1.09GB)
- The Elasticsearch data folder (data.zip – 18.5GB)
- Application source code (source_code.zip – 302MB)

The total size of all the files was approx. 20GB in size with the export being ready on 20th April.

Stage 4: Data Transfer to Intermediary Data Holder

Tim Evans emailed Andy a link to use a FTP site to transfer the data to the ADS on 20th April.

A second FTP site was required and Andy transferred all the files to the ADS on 20th April.

Stage 5: Check if data transfer is successful

On 21st April the ADS took the data from the FTP sites and loaded it into their servers running tests and checks on the data. On 23rd April Tim Evans emailed to state the transfer had been successful (after a couple of attempts transferring the large 18.5GB zip file) and that all checks had been carried out.

Stage 6: Reinstate the HER

Ben requested an FTP to download the data on 4th May. A link was sent to Ben on 27th May and the data was downloaded by Ben and placed on Warwickshire County Council's file system which is backed up. At this stage the destination HER would normally send a copy of their DMS (showing they have adequate ICT backup and security processes in place) to Historic England. For the purposes of this test Warwickshire already have a DMS fulfilling this part of the test.

Ben unzipped the files and all contents was checked.

One error was observed when unzipping the largest 18.5GB file (data.zip). The error appeared to relate to one particular .dim file in the zip folder. Only 223MB of data could be extracted from the 18.5GB zip file which suggests an error at some point of the data extraction or transfer process.

If the issue was a result of the data transfer process it raises the question of the appropriateness for using FTP for transferring large files.

The prospect of reinstating the Arches database was discussed by Ben and Andy and required the use of a PostgreSQL server. Although Warwickshire County Council did have access to some PostgreSQL servers, they were unfortunately not the right version needed to restore the backup of the Arches database (which needed PostgreSQL version 12). Warwickshire County Council ICT service identified that to set up a PostgreSQL server with the right version on their servers would take around 5 days of their ICT staff time. A potential solution was identified using a PostgreSQL server in Historic England's Azure Cloud Service, however after further discussion it was decided that it was sufficient to understand how theoretically the database could be installed and that it was not necessary to reinstate the database for the purposes of this test scenario.

One aspect that was identified from this discussion was the fairly large size needed to house the database and a substantial amount of time to restore and reindex the data (possibly 2-3 days).

Scenario 5 Result: test complete but not entirely successful.

4. Analysis and Discussion of Results

NSC1

Regarding the NSC1 aspect of the protocol the Project Team felt that despite most HERs not having a formal DMS, nor documentation of their hosts backup and security procedures, nearly all HERs carried out regular backups of HER data. Most HER hosts are local authorities and these follow fairly consistent guidelines and procedures regarding ICT data and security. In this respect it is felt a very basic level of data backup and security is in place but it should be formally documented and understood (in the form of a DMS) to be fully compliant with the NSC1 part of the Protocol.

Specific discussion regarding the DMS is covered below but in summary a number of ideas were put forward to how the DMS could be improved and these are set out in the recommendations section that follows.

It should be noted that there are many aspects of the DMS which are already well advanced by Historic England including:

- A recorded training webinar (https://youtu.be/8CTWkNRstxY)
- A dedicated webpage (https://historicengland.org.uk/research/support-and-collaboration/heritage-information-access-simplified/national-security-copy-nsc/)
- A DMS Template (https://historicengland.org.uk/content/docs/her/data-management-statement/)
- An annotated guide to completing a DMS (https://historicengland.org.uk/content/docs/her/guide-for-completing-data-management-statement/)
- FAQs
- DMS Exemplars

NSC2

Scenario 1 - Unitary HBSMR HER (Solihull HER) to County HBSMR HER (Worcestershire HER):

What went well

Simple to extract HER data, files and documentation. This appears to be mainly due to Solihull HER recently completing an audit, having an up to date HER database, good HER staffing and ICT support.

Data transfer to ADS and retrieval by Worcestershire HER went smoothly. This appears to be due to relatively small size of files, good network/internet connections and availability of key personnel at critical times.

Reinstatement of the Solihull HER was achieved relatively easily by Exegesis using their remote server with access given to Worcestershire HER.

What did not go well

Worcestershire ICT found it difficult to justify the time and staff resources to look at reinstating the Solihull HER on their own servers using their own ICT staff. They suggested a timeframe of many months would be needed.

Discussion

Some concerns were raised by the Worcestershire ICT service through discussions with the Worcestershire HER Officer:

- They had concerns about the security of the data (viruses etc) and trust levels with accepting data from ADS, lack of data sharing agreements. Also, whether there would be other information/checks required that they weren't aware of in application support.
- They suggested considering if local authority hosted HERs may be happier to receive data direct from another local authority rather than via a third party such as the ADS.
- They questioned whether a real scenario would involve just restoring a digital database or also other digital files and folders.
- They had concerns with running two separate instances of HBSMR on their remote desktop service (RDS), they suggested each pointed at a different database on different servers so that the database was always kept separately and questioned if they would ever want to be merged together.
- They wondered whether any staff at the Origin HER would still require access and who would need access at the Destination HER, would it need to be restricted? Either of these would add further complications around security groups, with delays if external access to internal RDS was required. They also suggested implications from a software licensing perspective.
- Concerns were raised regarding updating the databases contents to work with the Destination HER Front end/policies, would this cause issues if the database was ever returned to the host?

The Worcestershire Data Compliance Officer also had some suggestions:

- The Corporate Information Governance Team would need to be consulted about data sharing agreements, GDPR, who "owns the data".
- Data Processor agreement – agree to keep the data safe with appropriate security applied in line with origin HERs requirements, and, for any personal data held within the HER that we will be acting as a Data Processor to them and therefore only act on their instructions (and a raft of other clauses laid out in GDPR article 28). Data Processor Agreements are usually supplied by the Data Controller (in this case the origin HER).
- To make sure the origin HER data is kept separate from our own HER – we do not want to have to try to untangle a mix of both HERs later.

Scenario 2 - County Bespoke HER (Gloucestershire) to County HBSMR HER (Warwickshire):

What went well

Persevered with the test scenario to show what could happen in a real life scenario with a fairly uncooperative ICT service at the Host HER end.

What did not go well

Data Extraction was not carried out in the expected way with no simple backup or export of the HER database produced. Instead time-consuming and complex exporting needed to be carried out by the HER Officer with potential data loss/change.

Data Transfer was difficult and problematic due to both the size and complexity of the files. In the end only some of the data was able to be transferred.

Simple database reinstatement was not possible due to lack of completeness of data transfer and the complexity level to reinstate the HER database front end with the Destination HER service.

Discussion

This test scenario highlighted the need to have the availability of a cooperative ICT service to enable a full extraction or backup copy of the HER database to be produced quickly and easily in a time limited situation.

Compared to some of the other test scenarios the difficulty in reinstating the HER database with the Destination HER suggests this could also be encountered with other HERs that use bespoke HER software. Although the Gloucestershire HER documentation, including the DMS, did contain information relating to the HER database it was not enough information to restore the database without substantial conversations with the Origin HER Officer and ICT Service. Discussion with the Project Team on this matter suggested there could be other possible solutions to reinstating an HER service which would not necessarily mean recreating the bespoke software front end. One solution could be putting the exported Origin HER data into a different HER Software, this would involve substantial work on the data but could be achievable in a relatively short timescale (days) although would risk data loss or change.

Another aspect that this test scenario highlighted is issues with transferring the data by FTP. This failure to transfer all the data could be related to something as simple as poor or conflicting network/internet connection. However, there is also the possibility that the complex number and size of files and folders or even the subfolder structure itself was causing the FTP transfer to fail. Tim Grubb noted in particular that if the folder structure could not be retained this may have some implications for reinstating the HER at the Destination HER end.

A further benefit of carrying out this Test Scenario, even though it partially failed, was self-reflection by the Origin HER Officer. Tim Grubb mentioned that it was a useful exercise to highlight some weaknesses in his HER and to consider ways to improve documentation, internal backup and security procedures and what to consider if something like this needed to take place. He further went on to say that he would consider raising with his ICT service development time to build in an easy export function for the HER database. Manually exporting data had also highlighted some gaps in the HER documentation which should be resolved.

Scenario 3 - Trust managed HEROS HER (BaNES) to National Park HBSMR HER (Exmoor):

What went well

Data transferred successfully to ADS and retrieved by destination HER.

What did not go well

HER Database could not be reinstated by destination HER due to lack of ICT time/resources to use the HEROS front end software.

Discussion

There were few issues encountered with this Test Scenario. The reinstatement of the HER database was felt to be theoretically possible and highly likely to succeed despite not being able to be achieved for this test.

What this test scenario did highlight was the need for capacity by the right staff/experts and at the right time.

Scenario 4 - National Park HBSMR - remotely hosted (Exmoor) to County HER (Warwickshire):

What went well

Data compliance agreements raised and signed by all parties; this was helped by the Origin HER having a small dedicated ICT service where the ICT Officers role included being the host organisation's data compliance officer.

Data was transferred successfully to ADS and retrieved by Destination HER.

What did not go well

HER Database could not be reinstated by destination HER due to lack of compatible data servers.

Discussion

This test scenario highlighted that despite staff capacity and knowledge a final reinstatement could not take place due to a lack of software/server compatibility from the Destination HER. All parties expressed high confidence of successfully reinstating the HER if a compatible server was available.

Scenario 5 - Arches Database (Historic England) to County HBSMR HER (Warwickshire):

What went well

Information security and compliance was approved by the Origin Database holder.

Data was exported and appears to have been successfully transferred to ADS.

What did not go well

Long delays in initial discussions with Origin Database host.

Delays in transfer to data to ADS and for destination HER to retrieve and download the data.

Possible data loss or corruption at some stage of data export, zipping, transfer or retrieval.

Not able to test reinstatement of database as Destination HER did not have compatible data server version.

Discussion

This test scenario highlighted how a number of issues could easily delay and cause substantial problems in carrying out the NSC Protocol. Staff capacity led to a number of delays. The huge size and complexity of the files that were exported caused problems in being transferred, leading to assumed data loss/incomplete data being received by the Destination HER. Finally, incompatible server versions meant it was not possible to reinstate the database. These are all issues that need to be highlighted for anyone looking to enact the NSC Protocol.

General Discussion of Results by Project Team

To help frame the discussion relating to the results of the testing a series of questions were put to the Project Team:

- *Were roles and responsibilities documented within the Data Management Statement clear at the outset?*
- *Does the NSC DMS provide sufficient information and metadata to facilitate the process?*

In general, the project team felt that the roles and responsibilities were clear but there were some areas that could be improved in the DMS such as:

- GDPR: For the DMS to include a section to record how an HER treats their data under GDPR, i.e. what kind of GDPR classification does it fall under.
- Data Backups: To include all individuals (name or job title) of those involved in backing up HER data

Some HERs found it difficult to complete the DMS and wondered about the relevant of all the sections/questions.

Some questioned if the DMS template changes then how often should HERs update their DMS. It was felt that the DMS should be checked and revised annually and that this would include checking if a new DMS template was available.

- *Did other people need to be involved and at what stage was their engagement required?*
- *What constraints were encountered in respective of time/resource/ required level of skill and experience of those involved?*

The Project Team identified as a minimum the following people who should be involved if the NSC process was invoked:

  - Origin HER Officer
  - Origin ICT Service Personnel
  - Origin Data Compliance Officer
  - Third Party Intermediary Data Holder (e.g. ADS)
  - HER Software Company/Expert (e.g. Exegesis)
  - Historic England HIPs Team

It was felt that without these specific people available to take part in the NSC process it would be much harder to complete the transfer of data and achieve a successful result.

A Destination HER Service would not be necessary to ensure a copy of the HER data was secure, however it would be important that the Third Party Intermediary Data Holder ensured that the data transfer had meant no loss or errors in the data, this may involve unzipping folders and files and checking lists of files/folders against supplied documentation.

In theory a secure copy of an HER database could be made within a short timescale, just days if the right people are involved, are available and understand the process and what is trying to be achieved. However, in some cases this process could be delayed, questioned, agreements signing, professional staff booked in etc and could lead to weeks or months of time before a secure copy of the HER data was achieved.

For reinstatement of an HER database this has proved to be a much more complex and harder task to achieve and leads to all kinds of questions, options and issues. Data agreements and licences would need signing by multiple organisations, software versions and licencing may need to be obtained, specific staff and experts may need to be booked in and paid to work on aspects of reinstatement.

The question was raised by the Project Team about reinstating an HER database, is there a need? Many felt this should be tied into the reinstatement of an HER Service rather than to prove a copy of an HER database is secure.

- *How did people find the experience – what are their thoughts and feelings about interacting with the process?*

Most involved in the project found the data extraction and transfer relatively easy.

Some felt it was disappointing not to reinstate the HER database as this seemed to be the only sure way of telling if the data transfer had been successful.

It was clear to those involved in the project that the simplest option to ensure a secure copy of the data was to have it placed on an external server, leave the data in place and to grant access to those who needed it. However even then some pointed out there are risks such as losing keys, logins or passwords.

Many felt that to ensure the HER data was secure needed a combination of infrastructure expertise (i.e. software) and data expertise. Also, each HER service situation was different so there may not be a one size fits all solution.

Some felt that consideration should be given as to how documentation as a result of trigger events is held and accessed by all appropriate parties (e.g. web-based storage such as OneDrive/SharePoint etc).

- *What additional support, guidance and training may be required?*

Some felt more training and example DMS documents may help an HER when completing a DMS.

One area that could benefit from further support and guidance could be in helping HERs test their data backup and security procedures. Perhaps example testing scripts could be developed and form part of a regular process that HERs carried out

- *Where the HER provides service for more than one local authority, were there additional factors that needed to be taken into account?*

One area to take into account would be ensuring permission had been checked or obtained from data owners rather than those managing an HER.

Worcestershire raised an issue regarding access to a security copy of another HER, it would need to remain separate from other joint services, authorities or stakeholders.

- *Is there a need to rehearse the NSC process on a regular basis?*

General consensus from the Project Team was that a regular rehearsal process to test the NSC process would be beneficial. This would not only ensure that an HERs backup and security processes were tested but it could also lead to a regular security copy of HER data being produced and held by a third party if desired.

A simple HER backup and security test process could be carried out annually, perhaps as part of the Annual HER Survey, although it would need a careful balance of being rigorous but not heavily demanding on HER or other staff time.

A further suggestion was to fully test the NSC Protocol every 5 years as part of the HER Audit Cycle. This could include extracting a full security copy of HER data and sending it to a third party or Historic England to hold and maintain.

Although this would be highly beneficial it was felt this may not resolve issues from HERs that did not take part in the HER Audit Programme or who did not fill in the Annual HER Survey. It was also felt that these same HERs may be the ones most at risk of failure or loss of data and some form of targeted programme may be needed to ensure all HERs took part.

Reinstating HER databases:

Scenario 1 (Unitary HBSMR HER (Solihull HER) to County HBSMR HER (Worcestershire HER)) was the only scenario where the Origin HER database was successfully reinstated and accessible by the Destination HER. However, even in this case it required the intervention by Exegesis and the data was held on an external Exegesis server not the Destination HER's own servers.

For the other scenarios a combination of one or all of these factors led to reinstatement of the Origin HER not being possible:

- Lack of available compatible server software
- Lack of available front end software
- Lack of available ICT staff time/capacity
- Unsuccessful extraction of data to enable full reinstatement
- Unsuccessful transfer of data to enable full reinstatement

Reinstatement of an HER at the destination could also lead to other issues:

- What if the Destination HER then failed?

- What if the Destination HER unintentionally changed the data of the Origin HER due to different ICT/HER policies or procedures being used or different software or servers being used?

Any transfer process has risk of loss and degradation. The more you move data the higher the risk.

The difficulty in reinstating an HER database is in some ways due to the differences in software application being used. It could be argued that one way round this is to ensure all HERs can export their full HER data in a neutral cross compatible format such as MIDAS XML. However, practice within the HER community has shown that even when such a format exists it is not universally adopted therefore eroding this being a viable option for ensuring the NSC Protocol can be followed.

This difficulty in HER database reinstatement raises the question if there is a need to reinstate the database anyway, especially if we know the data has been transferred successfully.

Final Destination of Origin HER data:

Testing has shown that in most scenarios it was relatively easy to produce backup copies of HER databases with additional documentation including a DMS. It was also relatively easy to send this data to the ADS via a FTP. At this point it becomes a secure backup copy not held by the origin host HER service and it could be said that this fulfils the NSC Protocol entirely and there is no need to send the data to a destination HER host nor try to reinstate the HER database. The only scenarios where it was not easy to ensure an adequate backup copy of the HER was scenario 2 with Gloucestershire HER, who had problems both extracting the HER data and sending it to the ADS, and scenario 5 where there appears to be errors from the data transfer possibly due to the size of the data being transferred.

We know that the more parties involved in data transfer the more chances of issues arising including possible data loss, errors, complications etc. There is also a question whether the HER data needs to go to a destination HER anyway? For what purpose? We know that to reinstate the database is difficult anyway and that if the database is reinstated this brings into question all aspects such as data protection, data rights, data licencing, access to the data for both host and destination HER services etc. It would seem far better to keep things simple.

Post NSC Protocol:

In the scenario that an HER was failing so severely that it was felt data loss may happen and the NSC Protocol was invoked, once the data is backed up, this then leads to the question of what will happen to the failing HER. Although the NSC Protocol enables a secure backup copy of the HER database it does not cover all the other digital and physical data the HER holds. Although reinstatement of an HER was achieved as part of this test project, this would not normally be expected from the NSC Protocol and there is the question of what to do with an HER on the brink of total failure? Do we need a protocol for saving a failing HER? Including all the physical and digital HER holdings and an established plan to reinstate the HER service? It is beyond the scope of this project to consider how this may be possible but perhaps should be investigated as a further project in the future.

Data rights, copyright, GDPR:

One issue that has not been tacked in great detail by this project but has been raised a number of times is that of data protection and data rights. A series of questions need to be answered, and potentially legal agreements made, before data may be able to be transferred and this could add a substantial time element, not to mention a cost, to any transfer. For this project many of these issues were dealt with simply and easily because it was just a test but in a real life situation it could get complicated and even halt the NSC Protocol process taking place.

If we consider that Data Protection Impact Assessments (DPIA) should take place before any data transfer takes place we found three main approaches from HERs taking part in this project:

Informal: Where some HER officers were able to decide themselves with their own training and authority the risk level of transferring data as part of this project. The fact that this was a test project carried out by a local authority funded by a national body and involving other local authorities and trusted partners meant that the risk level was considered low and the data being transferred was also considered low sensitivity.

Formal without signed agreements: This approach consisted of HER Officers asking permission from senior officers and ICT staff in their host authority who authorised the data transfer without a formal agreement needed. The fact that this was a test project carried out by a local authority funded by a national body and involving other local authorities and trusted partners did influence this decision by a host authority.

Formal with signed agreements: This approach was where the host authority insisted a formal Data Protection Impact Agreement was in place and signed by all parties before any data transfer took place.

It was felt that if this was a real life scenario the only acceptable approach would have been the latter with formal signed agreements by all parties.

Higher Risk HERs

The testing has shown that the most difficult HERs to enact the NSC Protocol appear to include one or more of the following:

- HER uses bespoke HER database software
- HER has difficult relationship with host ICT Service
- HER does not use remote server hosting for HER database
- HERs with limited capacity and resources for ICT service
- HERs with limited capacity and resources for HER staff

5. Recommendations

This project has shown that it is possible to follow the NSC Protocol and achieve a security copy of an HER held by a third party relatively easily and in some cases even being able to restore that database with another HER. However, in some cases it has proved difficult to extract a copy of the HER database, difficult to send a copy to a third party and not possible to reinstate the database with another HER. Analysis and discussion has raised a number of points that should be resolved or clarified if the NSC Protocol is to be successful. What follows are a series of recommendations for Historic England and the HIAS Programme to consider with the aim of improving and ensuring the NSC for HERs can be achieved.

NSC1

For the NSC1 the focus is on security and backup of data by host HER authorities and ensuring adequate documentation exists in the form of a Data Management Statement (DMS). For the first aspect, in terms of security and backup of data, we know a basic form of backup exists with most, if not all, HERs. The focus instead should be on ensuring adequate testing and documentation of these processes. Some of these aspects are dealt with as recommendations below in the NSC2 Recommendations, what follows are recommendations related to the DMS itself.

DMS

Recommendation 1: **Suggested Revisions to the DMS Template:**

- Include a section on GDPR for an HER to record how they treat their data under GDPR and other copyright and information management legislation
- In the 'Digital Data Backup' section to include all individuals (name or job title) of those involved in backing up HER data

Recommendation 2: **Annual revision of DMS by HERs**

The DMS should be checked and revised annually including checking if a new DMS Template is available

Recommendation 3: **Links to software provider documentation**

For HERs which use the same HER software then common aspects of the software could be provided in one online location by the software provider fulfilling many aspects of the documentation (e.g. database entity relationship diagram or system requirements).

Recommendation 4: **DMS Training and Support for HERs**

For Historic England to continue the excellent work they have done to date in supporting HERs in completing a DMS including websites, webinars, templates, exemplars etc.

NSC2

Recommendation A**: Clarify Purpose and Status of the NSC and the NSC Protocol**

All parties involved in developing and agreeing to the NSC should clearly understand that the NSC is only to be used as a security backup process and that enacting the NSC Protocol will only be in an essential emergency situation where an HER appears to be failing and data loss may be imminent. It should not

be used to restore a failing HER service nor change or move an HER service from one authority to another.

Recommendation B: **Clarify Destination of Security Copy of HER data:**

The NSC should only require a copy of HER data and documentation to be held by a trusted third party such as ADS or Historic England. The database does not need to be reinstated or used in any way as the intention is for it to be a secure backup copy only.

Recommendation C: **Ensure a DPIA (Data Protection Impact Assessment) is carried out as part of the NSC Protocol:**

A formal DPIA should take place by the host HER authority, with formal agreements signed by all parties needed to enact the NSC Protocol, before any data transfer takes place.

Recommendation D**: Regular production of security copies of HER data**

Consider establishing a regular programme of taking security copies of HER data to be held by a trusted third party. This could be part of the HER audit programme so that a security copy of an HER database is taken every 5 years. Another possibility is for HER software providers to ensure this happens as part of their Annual Service Visit/Procedures.

Recommendation E**: Regular testing of HERs inhouse data backup and security process**

Establish regular annual testing of HERs inhouse data backup and security procedures, possibly as part of the HER Annual Survey or alternatively as part of HER Software Providers Annual Service Visit/Procedures. A simple test script could be developed with the results documented by HERs and forwarded to HE as part of the Annual HER Survey and HER Audit.

Recommendation F**: HERs move to Remote Server based HER Software and Data Storage**

All HERs should consider moving to a remote server based HER Software and Data storage system as this provides the easiest and most robust method of ensuring the NSC Protocol can be followed if needed.

Recommendation G**: Target High Risk HERs**

Consider targeting those HERs that appear to be the highest risk of data loss, being unable to participate in the NSC or being unable to enact the NSC Protocol if needed. Criteria could be developed to identify higher risk HERs including those HERs that:

- Use bespoke HER software
- Do not have an HER DMS

- Are not active in the HER Audit Programme
- Have no dedicated HER staff
- Provide no evidence of continuous backups (annual, testing)
- Not adopted by host authority

These HERs should be specifically targeted to ensure a security copy of their HER database (together with any appropriate documentation) is transferred and held by a trusted third party.

Other issues for consideration

Other HER data:

Some thought and consideration should be given about what to do with all the other information, both digital and physical, held by HERs. If an HER were to fail completely this information would be as valuable and as essential as much as the basic digital HER database is. Other digital data held by HERs could be many Terabytes in size and would probably need alternative methods of data transfer than simple FTP or file sharing. There would probably need to be some form of bespoke arrangement to transfer the digital and physical data involving visiting physical offices and retrieving physical and digital data on and off site. Collection, transportation, storage and management and maintenance of all the physical and digital data of an HER will have a substantial cost and staff resource implication. Some further work could be done to establish what the total average physical and digital holdings of HERs are and calculate some costs to collect, transport and store this including staff costs. Needless to say, some thought would also need to be given to the copyright and GDPR implications of passing over all the physical and digital information to a destination host or third party.

Reinstating a failing HER

Although this project has tested and learnt a lot regarding moving HER data from one authority to another, including consideration of other physical and digital data that HERs hold, It has not been able to significantly test options, nor scenarios for transferring or reinstating a whole HER service. However, just from this project alone with the limited scenarios, HERs and testing involved it is clear that transfer and full reinstatement of an HER service would require a substantial bespoke assessment and solution and could be very different every time.

Consideration should be given to a project to explore how to fully reinstate failing HERs with detailed recommendations and time and cost implications.

Likely costs and resources needed if the NSC Access Protocol is initiated.

Below is a breakdown of the resources and costs expected if the NSC Access Protocol is initiated. All times and costs are approximate and will vary depending on the HER circumstance and exact method of transfer used.

Host HER:

- In house HER staff time: 1 - 2 days (£300-£600)
- In house ICT staff time: 1 - 2 days (£300-£600)
- In house data compliance officer time: 0.5-1 day (£150-£300)

Third Party Data Intermediary (e.g. ADS):

- Staff time: 0.5 days (£250)
- Data storage costs (1TB): £5-10 per month

Historic England:

- HIPs (or equivalent) staff time: 1 day (£300)
- Data storage costs: £5-10 per month

Specialist Software Provider

- Staff time: 0.5 days (£300)

Total cost: Approx. £1500-2000

Total time needed: min 1 week, up to 1 month

6. Conclusion

This project sought to test how far the NSC Code of Practice and Access Protocol could be followed in a real world situation. It took a number of different scenarios and pushed each test as far as possible to achieve all aspects of the protocol including data extraction, transfer and reinstatement as well as considering documentation and other aspects.

In some ways we can consider the project to be a great success as it achieved the original objectives set out and even when some scenarios failed to be completed through to the end of their testing, a lot was learnt and documented.

Detailed analysis and discussion have allowed a series of recommendations to be made from this project and the next stage is for these to be considered by the HIAS NSC Workpackage to establish the next steps for the NSC.

Appendix A: Test Script

Test Script 1.0

(To test NSC2 Stages 2 to 4)

A note about documentation:

All email communications relating to testing should copy in the Project Manager (Ben Wallace).

Please keep a note of any conversations, discussions, decisions etc that are made relating to the project. These should be sent to the Project Manager when each test scenario has finished.

For each stage of the Test Script please record (within a Word document copy of this test script) how you followed each stage and the result as well as any points to note, comments, ideas etc. Dates and times should be recorded as well so we can see how long each stage takes. These should also be sent to the Project Manager at the end of each test scenario.

Start of Test Script

Stages:

1. **Stakeholder Consultation**

   Early dialogue between all parties determined necessary when the Access Protocol needs to be invoked. This would probably be:

   - Origin Host/Service HER
   - Origin Host ICT Service
   - Destination Host/Service HER
   - Destination Host ICT Service
   - ADS (as intermediary data holder)
   - Exegesis (if either HER uses HBSMR)
   - Historic England (primarily HIPs team)

   Agreement on all aspects of the process needs to be reached by all stakeholders before the next stage can start.

2. **Initiate Access Protocol**

   In the current NSC2 process this would normally be carried out by Historic England. However, for the purposes of this project, this will be undertaken by the Project Manager who will contact the Origin HER to start stage 3 of the script.

3. **NSC preparation for transfer**

   At this stage, the Origin HER (and/or their ICT Service) prepares a copy of their HER data along with supporting documentation and resources (policy documentation, DMS, index to HER's reference collection etc). When this is ready the Origin HER emails the ADS (in this case Tim Evans) to notify

they are ready to transfer data and request the details of the FTP. Ideally the Destination HER should be copied into the email so they know the process has been started. Within this email the Origin HER should include the DMS and details of the files that they are looking to transfer, as a minimum the ADS would like to know the number and total size of the files and ideally a list of files and folders to be transferred. One method of producing a list of files and folders within a Windows folder location is detailed here:

- Windows key: Type "command"
- Run Command Prompt App
- Type "cd", then space, then paste the file path of the folder, then enter
- Type "dir /s"
- The resulting text can be selected by dragging the mouse over it or (more safely) by pressing 'Ctrl' + 'A'
- Copy this text ('Ctrl' + 'C') and then paste it into a blank Word document to attach to the email

For the purposes of this project the files to be transferred should be all those related to the HER digital database and spatial data needed to reinstate the HER as a functioning database as well as significant HER documentation as listed within the HER Audit Specification (DMS, HER manual, HER policies etc).

If possible, it would be beneficial for each Origin HER to email the ADS an approximate potential file size of all other digital HER data (digital reports, aerial photos etc). This would help us understand the potential scale of transferring other HER data not directly related to the HER database. If no index of physical sources held by the HER exists it may also be useful to include a brief summary of physical sources the Origin HER holds as well.

4. Data Transfer

ADS will email the Origin HER the details of the FTP to use to transfer the HER data and the Origin HER should then transfer the data to the ADS and notify the ADS by email when this transfer has taken place.

5. Check if data transfer is successful

ADS will absorb the data into their systems ensuring it is checked for any loss or issues from the transfer and that it is secure and backed up accordingly. The ADS will email the Origin HER to notify them the transfer has been successful and that the data has been checked and backed up.

6. Reinstate the HER

For the purposes of this project we are testing reinstatement of the Origin HER with a Destination HER Service. This can have a number of sub-stages but as a minimum will involve the following:

a) ADS emails the Destination HER to inform them that they can now receive the HER data using FTP (with details of the FTP being supplied to the Destination HER within this email). The ADS would include the list of files and folders they should expect to receive as per the Origin HER's first email.

b) The Destination HER receives the data and confirms back to the ADS that it has been received and that the data is now secure and backed up as per the Destination HERs ICT protocols. At this stage the Destination HER should send details of their ICT data security and backup procedures to the Project Manager (acting in the place of Historic England) and the ADS, this could be in the form of a DMS.

According to each scenario the following sub-stage may not be possible but ideally should be attempted and if not possible to test reasons should be recorded as to why this sub-stage could not be tested:

c) Reinstate the HER using appropriate software and servers and then access and export some of the HER data to prove this. Exports could be in the form of CSV, XML, PDF and made of single or multiple records such as Monuments, Events or Sources. Additional exports of GIS data could be carried out. Screenshots could be taken to show reinstatement of the HER database and GIS.

7. Deletion of security copy of HER data

Once stage 6 has been completed then the Destination HER should email the ADS to say that the HER data held by the ADS could now be deleted. For the purposes of this project the data will continue to be held by the ADS in case further testing needs to take place. Before the end of the project all copies of HER data held by the ADS and Destination HERs will be deleted, an email will be sent by the Project Manager to notify when this should take place and to confirm it has been carried out.

End of Test Script

Notes: