National Security Copy

Access Protocol

Overview

The Access Protocol (AP) sets out the process for depositing the National Security Copy 2 (NSC 2) with a third-part service for safekeeping. It is governed by the best practice principles of the National Security Copy Code of Practice (NSC CoP) and the Data Management Statement (DMS) which covers the creation of the National Security Copy 1 (NSC 1) through routine backing up of data.

This Protocol relates to the Heritage Information Access Strategy (HIAS) Principles 6 & 7, which state that "data or knowledge should not be at risk of loss, fragmentation, inundation (in data), or system obsolescence" and "Historic England should, on behalf of the nation, ensure that a security copy of all such data exists".

The Access Protocol outlines how the exceptional decision to deposit a security copy of a heritage dataset with another heritage organisation for safekeeping should be done. Enacting the Protocol will only be essential in emergency situations, it should not be used to restore a failing Historic Environment Record (HER) service nor move the HER service from one authority to another.

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.

The Process

The National Security Copy 2 is currently broken down into four stages of implementation:

Stage 1: Assessment of risk in response to a Trigger Event.

Concerns over the stability of an HER's IT system or infrastructure, and/or the financial/resourcing and sustainability of an HER service may spur a Trigger Event such as where:

- an existing database is unstable and is being moved to a new system; and/or
- a reduction in staff and/or expertise falls to a level where the organisation can no longer ensure that best practice is being followed, or 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 should inform Historic England of the situation (or Historic England is notified by other means); and
- Historic England shall assess the risks and support the local authority to manage the situation (the DMS requires details of non-HER local authority contacts for this purpose, in addition to the HER contact).

The assessment by Historic England reveals either:

- The risk to security of the data is **low** and the situation can be managed in-house by adhering to best practice as set out in the HER's DMS and the NSC Code of Practice. Historic England will continue to monitor the situation; or
- The 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 best practice is being followed and responsibility is maintained). The process then moves to Stage 2.

Stage 2: Stakeholder consultation

To implement the Protocol, stakeholder consultation must take place; stakeholders may include ALGAO (England), neighbouring historic environment officers, and other bodies such as local archives and museums. Following consultation and stakeholder agreement, Historic England shall initiate the implementation of the AP. Once the Protocol has been invoked, Historic England will oversee the process, negotiate permissions, and, if necessary, commission a third-party service to manage the technical stages of the transfer.

Stage 3: NSC 2 preparation and transfer

A security copy of the data is taken, following the guidance in the organisation's DMS, and transferred to the appointed host.

- A security copy of the data is prepared for transfer, along with supporting documentation and resources (in particular, policy documentation, including the DMS and an index to the HER's reference collection).
- If HERs do not already have a Data Protection Impact Assessment (DPIA) that specifically covers transfer to a third party, then one should be drawn up based on the host authority's template and signed by the relevant parties — even if no personal information covered by GDPR is held in the HER.
- A third-party intermediary host is appointed by Historic England.
- The security copy and supporting resources are transferred to a temporary safeguard. On-going storage and security maintenance of the data is enacted 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 AP 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.

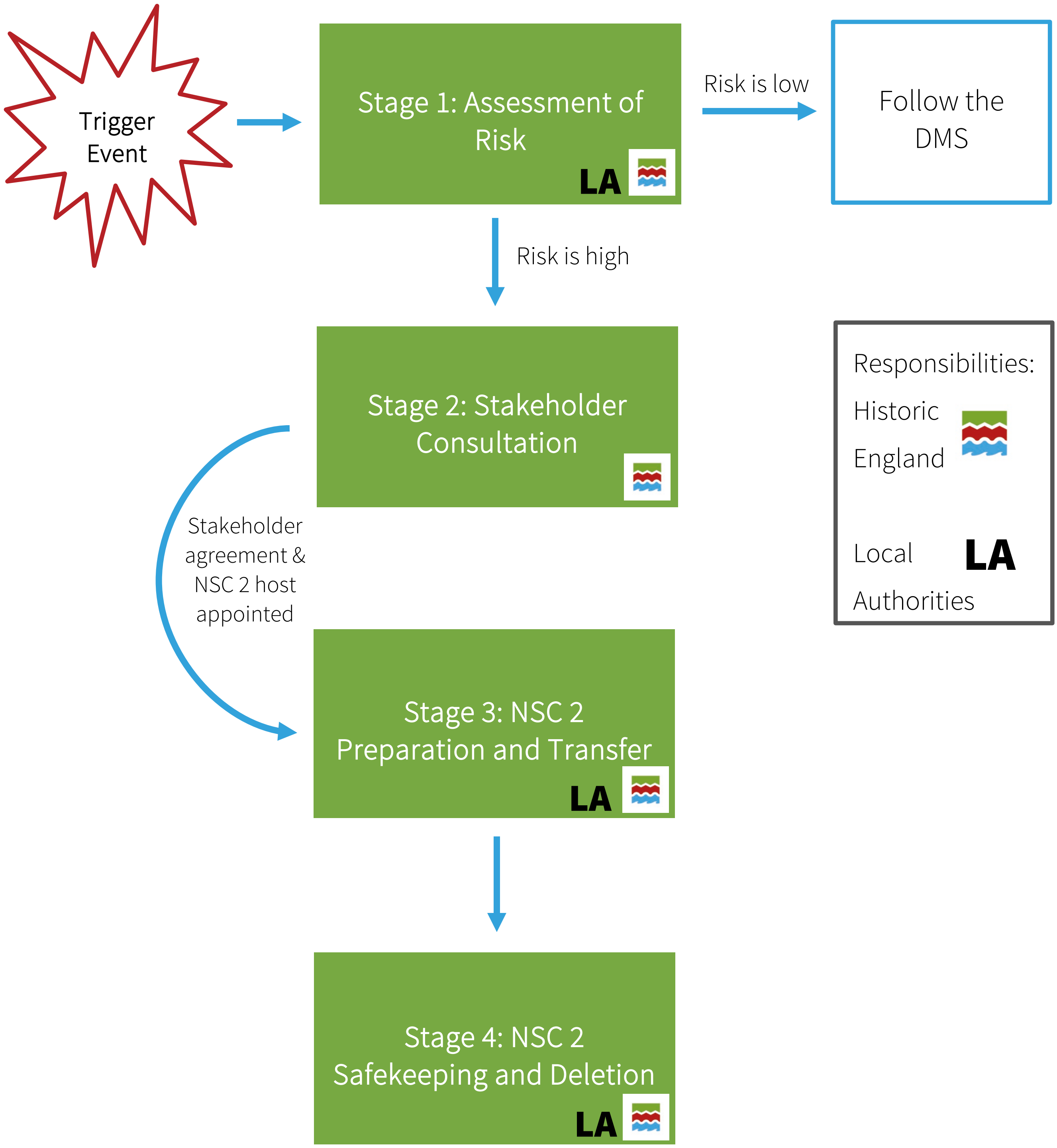
Stage 4: NSC 2 safekeeping and deletion

The NSC 2 is a copy of HER data held as security against loss or corruption during a Trigger Event. In most 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.

Although it is not the purpose of the security copy, in exceptional situations the copy itself may be transferred to a new host.

Flow Diagram of the Access Protocol Process



Trigger Event

Stage 1: Assessment of Risk

LA

Risk is low

Follow the DMS

Risk is high

Stage 2: Stakeholder Consultation

Stakeholder agreement & NSC 2 host appointed

Stage 3: NSC 2 Preparation and Transfer

LA

Stage 4: NSC 2 Safekeeping and Deletion

LA

Responsibilities:

Historic England

Local Authorities LA