Company Records Policy

This policy applies to everyone, including consultants and those on temporary contracts.

Coverage: This policy covers the information produced by Highways England which qualifies as a business record. It does not cover information held on Personal Workspaces in SHARE, information held in Outlook, or paper documents not kept on registered files. It does not cover any information retained on legacy group drives or personal drives or on any form of removable media.

Purpose: You must apply this policy whenever you create, hold, review or dispose of information (in whatever form or medium) that might form part of our company record. Observing this policy will ensure that you and the company meet a range of legislative and regulatory provisions covering record keeping and access to our records. This policy applies throughout the company.

Your responsibilities

We are all responsible for:

- Deciding what information should become an official record.
- Keeping records in the recognised records management system for the type of information e.g. property records in HAL, Geotechnical in HAGDMS, etc. and in the appropriate place within those systems.
- Seeking advice from management, process owners or the Company Record Officer when necessary

Process Owners are responsible for directing colleagues about

- records to be kept of decisions/actions taken when following their process;
- At what stage in the process documents become records;
- Where the records for their process are to be stored

Information Policy

Records must be kept in the appropriate system for its format – see below. Every record will be retained for a set period after which it will be either:

- destroyed, or
- if kept for 20 years, be reviewed and either
    - retained for a further period,
    - transferred to the National Archive or

- destroyed.

These periods are agreed between the business area and the Company Records Officer.

Electronic records must be held in the approved system for the class of record. Approved electronic records management systems are:

Confirm: for asset delivery records

ControlWorks: for traffic management records

HAL: for records relating to land ownership and property management

HAGDMS: for geotechnical records

IAM IS: for asset management records

PfP: for HR and Finance records

SHARE: for documents and records of policies, projects, and procedures

Other shared electronic systems may not meet with the standards for electronic records storage. Where electronic records cannot be saved into SHARE the company records officer will agree the method of storage with the business area.

Paper records must be kept in the registered filing system managed by your local Records Management Unit. Physical files will only be provided in the following cases:

- Where the records you need to keep have arrived in hard copy format from an external source and scanning facilities are unavailable.
- Where the records are electronic but stored on removable media and are unsuitable for loading into SHARE
- Where the protective marking for the information is SECRET or TOP SECRET
- The records are concerning the Historical Rail Estate

If you handle material classed as Secret or Top Secret you MUST consult our IT Security Officer for advice on secure storage and handling

Where records on a single subject are in both electronic and hard copy (for the reasons above) the business area should maintain records in the appropriate system and cross reference between the appropriate system, e.g. SHARE and the registered file.

For records in other media, please consult the Company Records Officer.

Paper records considered vital to business continuity should be protected by storing copies in a separate location. The Company Records Officer can advise on the provision of special storage.

Disposal of Information

Both paper and electronic records must only be deleted in accordance with the agreed retention schedules. Documents that have not yet been declared records may be deleted by the owner, or by an Information Manager. If in doubt, you should consult your Information Manager before doing so.

Malicious deletion or destruction of information from any of our records systems is misconduct which will attract disciplinary action. Such action may also be unlawful and will render the individual liable for prosecution. Draft copies of information should be deleted once a final version has been agreed.

Extract from Freedom of Information Act 2000 Part VIII section 77:

" where a request for information has been made... under this Act or the Data Protection Act, any person...is guilty of an offence if he alters, defaces, blocks, erases, destroys or conceals any record held... preventing the disclosure of the information ....."

This applies to any information held by us in any format, and does not apply only to information declared as a business record.

DOCUMENT CONTROL

Title	Company Records Policy
Author	Stephen Bagley
Owner	Stephen Bagley
Date	June 2019