SCOPE

Balfour Beatty Plc and its group companies in the UK ("the Company") are committed to ensuring that records are created which are capable of supporting business functions and activities for as long as they are required through good Records Management practices. This policy applies in relation to the Company's UK operations. N.B. the Company's overseas subsidiaries and group affiliates may implement their own local records management and retention policies from to time to time, to comply with local law requirement in their respective territories. This policy has taken into account the operational, legislative, and regulatory and accountability requirements for records management. All employees, permanent or temporary, and those working on behalf of the Company including agency staff and/or consultants have a responsibility to effectively manage the Company's paper and electronic records in accordance with this policy so that it supports efficient working practices and meets the Company's legal responsibilities. This policy must be read in conjunction with the Retention Schedules and the Balfour Beatty Data Protection Policy.

PURPOSE

This policy sets out the Company's approach to records management and provides the guidelines for all employees to follow to ensure they are clear about the policy and are able to carry out their work in accordance with its requirements. Please also reference SBU specific Records Management procedures for filing structures and SBU specific amendments.

Associated Documents

LGL-RM-0043a	Document Retention – Accounting and Tax Records
LGL-RM-0043b	Document Retention – Companies Act Records
LGL-RM-0043c	Document Retention – Employment and Pension Records
LGL-RM-0043d	Document Retention – Information Management Records
LGL-RM-0043e	Document Retention – Insurance Records
LGL-RM-0043f	Document Retention – Intellectual Property Records
LGL-RM-0043g	Document Retention – Meeting and Minutes
LGL-RM-0043h	Document Retention – Pre-qualifications, Tenders and Contracts
LGL-RM-0043i	Document Retention – Property Records
LGL-RM-0043j	Document Retention – Quality Assurance Records
LGL-RM-0043k	Document Retention - Shares and Dividends Records
LGL-RM-0043l	Document Retention – Safety, Health and Environment Records

1. Roles & Responsibilities

1.1 Key roles within the Company in relation to information management and data protection compliance and the responsibilities of these roles and of all employees in relation to such matters are outlined in the Balfour Beatty Data Protection Policy.

2. Record creation and maintenance

2.1 Balfour Beatty Strategic Business Units (SBUs), Business Units and functions are expected to ensure that records are created that document their respective activities, as well as ensuring that:

- Records have an owner i.e. an author or document creator
- Records are named correctly, with the use of appropriate and approved naming conventions, which may be locally agreed.
- Metadata is applied to the records such as; author, date created, version, protective marking classification, subject etc.
- Staff are appropriately trained in the use of systems they are authorised to access and have access to user manuals
- Appropriate protection and access controls are applied where necessary.
- Systems and records are kept accurate and up-to-date
- Records are not retained longer than necessary, and are retained in line with the relevant legislation and the retention schedules.
- Non-current records are archived and properly indexed to indicate the type of records they are, whether they contain commercially-sensitive or confidential information or personal data and the relevant retention period to ensure that they are retained in accordance with the relevant retention schedule, records that have passed its retention period is disposed of in a controlled and where necessary in a secure manner.
- Work related records and information are not saved on personal drives, but are stored in a shared team area with access restricted to authorised staff.
- Current records are arranged in such a way that they can be retrieved quickly and efficiently, such as in a corporate approved file plan.
- There is an audit trail of the movement and location of records so that it can be tracked and monitored so that that they can easily be retrieved. • Adequate storage accommodation is provided for hard-copy records
- Electronic and paper records are cross-referenced where possible.
- Vital records are identified and are appropriately protected for business continuity purposes and an appropriate business continuity plan is in place to protect the vital records.
- Information Risks assessments are carried out on Information Assets and records, so that risks to the records or Information Asset are appropriately managed.

3. Record retention and disposal

3.1 A series of “retention schedules” set out the recommended retention periods for different classes of documents. These schedules cover documents in key areas including Companies Act records, accounting and tax, employment and pensions, SHE, contracts, tendering documents and property records. The retention schedules are intended to enable users of this document to simply refer to

the relevant retention schedule that covers the particular class of document that they are interested in and then determine the relevant retention period from that schedule. If a document is not covered by any retention schedule, reference can be made to the items listed in below in determining an appropriate retention period. SBUs/functions may wish to refer to these retention schedules and the general guidance below in reviewing their current existing document retention and disposal practices. The DPO within the SBU/function has the responsibility for establishing and implementing effective practices and procedures across it to give effect to this document.

4. Recommended Retention Periods

4.1 The recommended retention periods (set out in the schedules) take into account minimum retention periods specified in legislation, limitation periods, the requirements of the Data Protection Act 2018 (subject to royal assent) ("DPA") and the General Data Protection Regulation 2016/679 ("GDPR") (together the “Data Protection Laws”) and current principles of “best practice” published by the Institute of Chartered Secretaries and Administrators. “Best practice” may mean that for certain documents the retention period is longer than the statutory minimum retention period.

Any document falling into two or more categories should be retained for the longer of the recommended periods.

Where the document to be retained does not fall within any of the retention schedules, the following factors may assist to determine an appropriate retention period:

- Documents should be retained until the risk of claims or litigation (if any) to
- which that document may be relevant has become time-barred under the
- relevant limitation period;
- Where there is little chance of litigation, the retention period should be
- proportionate to the length of time for which that document may still be useful
- for a legitimate business need;
- Where the information includes personal data, the requirements of the Data Protection Laws should be followed, namely, the personal data should not be retained in a form which permits identification of the data subject for longer than is necessary in relation to the purpose for which it was originally obtained (i.e. there must be a legitimate business reason to retain the personal data and only the minimum that is necessary for this purpose should be retained). Further information on this can be found in Balfour Beatty’s UK Data Protection Policy and the guidance document referred to in that Policy;
- Whether the document may be needed to enable us to respond to investigations by external agencies;
- Whether the document may be needed for any current or potential enquiry by HMRC into our tax returns (further information is set out in the attached accounting and tax records retention schedule);
- Where the documents are audit working papers, the requirements of the Group Audit Manual must be followed;
- Whether the document may be needed for any contractual reasons, such as an audit that

customers of Balfour Beatty are contractually (e.g. under a strategic alliance) entitled to undertake;

- Whether the document may be required to prove compliance with a regulatory requirement;
- Whether the document might be needed as evidence in legal proceedings; and the historical value of the document (if any).

4.2 The existence or contemplation of litigation (civil or criminal) or a regulatory investigation or external audit overrides the recommended retention periods. All documents which may be relevant for pending or actual litigation, regulatory investigation or audit must be retained regardless of the fact that under the relevant retention schedule, they may ordinarily be disposed. Any deliberate decision to destroy documents relevant to pending, threatened or ongoing legal proceedings or to a regulatory investigation may fall within the serious criminal offence of perverting the course of justice which potentially carries a sentence of imprisonment. Adverse inferences about Balfour Beatty's behaviour may be drawn by the court or investigator.

5. Electronic Retention of Documents

5.1 Where indicated in the retention schedule, documents may be stored electronically. Care should be taken in converting (and then storing) original documents to electronic versions as it may be necessary to rely on the electronic record as evidence in court, either when bringing or defending a claim.

Scanned and electronic imaged documents will generally be accepted by a court if it is satisfied that the original document existed, that the copy is complete and legible and that the copying and storage procedures were correct. Computer records are acceptable evidence on similar conditions and provided they can be converted into a satisfactory legible form. Note that the British Standard Institute (BSI) has published BSI Standard 10008:2008 regarding the electronic retention of documents. While BS 10008 is not legally binding and compliance with it will not guarantee that an electronically stored document will be admissible, BSI 10008 does provide a framework for a court to work within when deciding whether an electronically stored document is admissible in evidence. SBU/Functions may therefore wish to refer to BSI 10008 when storing documents electronically.

Where the law requires the retention of an original document (e.g. certificates of title to property, bank guarantees or performance bonds) it is not acceptable to scan the original to create an electronic record and then destroy the original.

Retention arrangements for electronic records should ensure that they will remain complete, unaltered and accessible throughout the retention period. Back-up copies of electronic records should be regularly taken and stored off site. Information retained only in electronic or digital format should be retained for the same period as it would be kept if in paper form.

6. Disposal of Documents: General Principles

6.1 Documents that have passed their retention period should not be retained and the

decision to dispose of them should be carefully made after consideration of the factors above.

As highlighted above, regard must be had to the requirements of the Data Protection Laws. This means that where documents contain personal data, such personal data must only be retained in a form which permits identification of the data subject for as long as is necessary to fulfil the purpose for which it was obtained. Once such personal data is no longer needed for a specific purpose, it must be deleted.

The decision to dispose of documents stored off-site with an external provider should not be left to the storage provider. Reasons may have arisen between the date when the documents were first archived and the proposed disposal date that mean that those documents now need to be retained for longer.

A record should be kept of documents stored off-site by an external provider that are then approved for disposal after the review process described above (including the method and date of their disposal).

Disposal of documents should be conducted in a safe, secure and responsible way (such as by shredding or disposal in a confidential waste bin) having regard to the confidentiality of the documents that are to be disposed. Documents that contain material that was highly sensitive when originally created but which are no longer required to be retained under this policy, may still require secure disposal if they may still be of general interest to a competitor.

7. Access

7.1 All employees and those who are working on behalf of the Company should ensure that they only access the information or systems if they have a valid business reason to do so and/or that they are entitled and permitted to see, in particular where it concerns personal data or sensitive personal data.

Accessing records or information outside of permitted access levels must be authorised by the Information Asset Owner and the reason for access must be recorded by the Information Asset Owner.

The organisation needs to ensure that any decisions regarding access to records are documented so that they are consistent, can be explained and referred to. Managers must ensure that:

- Employee access levels to information is agreed and identified in their network or system profile when joining a team or project.
- Decisions regarding amendments to access are documented

8. Data Subject Requests

8.1 All data subject requests (including subject access requests and requests for erasure) should be sent to dataprotection@balfourbeatty.com

9. Contacts

9.1 If you are unsure about how to comply with this policy or for advice on Records Management please contact the Group Data Protection Officer on telephone 0203 810 2590 or email Daniel.sullivan@balfourbeatty.com