



Subject: <b>Document and Data Control</b>	Number: <b>POL00102</b>
Approved by: <b>Managing Director</b>	Type: <b>Policy</b>
	Effective: <b>February 2021</b>
	Revision: <b>2.1</b>
	Effective: <b>October 2023</b>

### 1. Objectives

The purpose of the Document and Data Management policy is to establish the controls necessary to identify, maintain an effective manage the information, data and records that support the business.

Like every business, we use data and records to support many day-to-day operations. This information must be accurate, up-to-date and accessible to appropriate users. It must also be secured and protected to prevent unauthorised or inappropriate use.

Data and records take many forms. Data may be encoded within an information system, requiring some level of processing to translate the raw data into meaningful information. However, data may take other forms such as the documentation, work products and records supporting the organisation’s processes. Appropriate controls are therefore be applied in all cases to ensure that the integrity, configuration, storage, preservation and availability of data are appropriate and effective.

It is essential to treat information as a vital company asset and to ensure that it is fit-for-purpose, effectively managed and secure, irrespective of its source.

The document and data management policy defines the necessary controls to ensure that documents, data and records are reviewed for accuracy and completeness, while providing suitable storage facilities. Changes to documents and data are formally managed and controlled through configuration management systems. Archived data is secured in such to ensure that it can be retrieved if required. Obsolete data and records are destroyed to prevent potential misuse.

Records provide evidence of organisational activities. The effective management of records is essential, not only to provide regulatory bodies and customers that requirements and expectations have been met, but are also underpin effective management of the organisation, as they provide essential information about the activities taking place within the organisation, along with its performance.

The definition and management of appropriate process records is also critical to any performance improvement programme. Without data and records there can be no performance baseline as a starting point for improvement and no measure of the progress being made. In this situation any improvements that are achieved will be informal and ad-hoc and will be unlikely to be sustained.

### 2. Scope and Applicability

This policy applies to all documents and data that are maintained under formal release, configuration and change control. These include, but are not limited to:

- policies;
- procedures;
- operating standards;
- student records;
- HR records;
- operational data;
- employee data.



3. Procedure

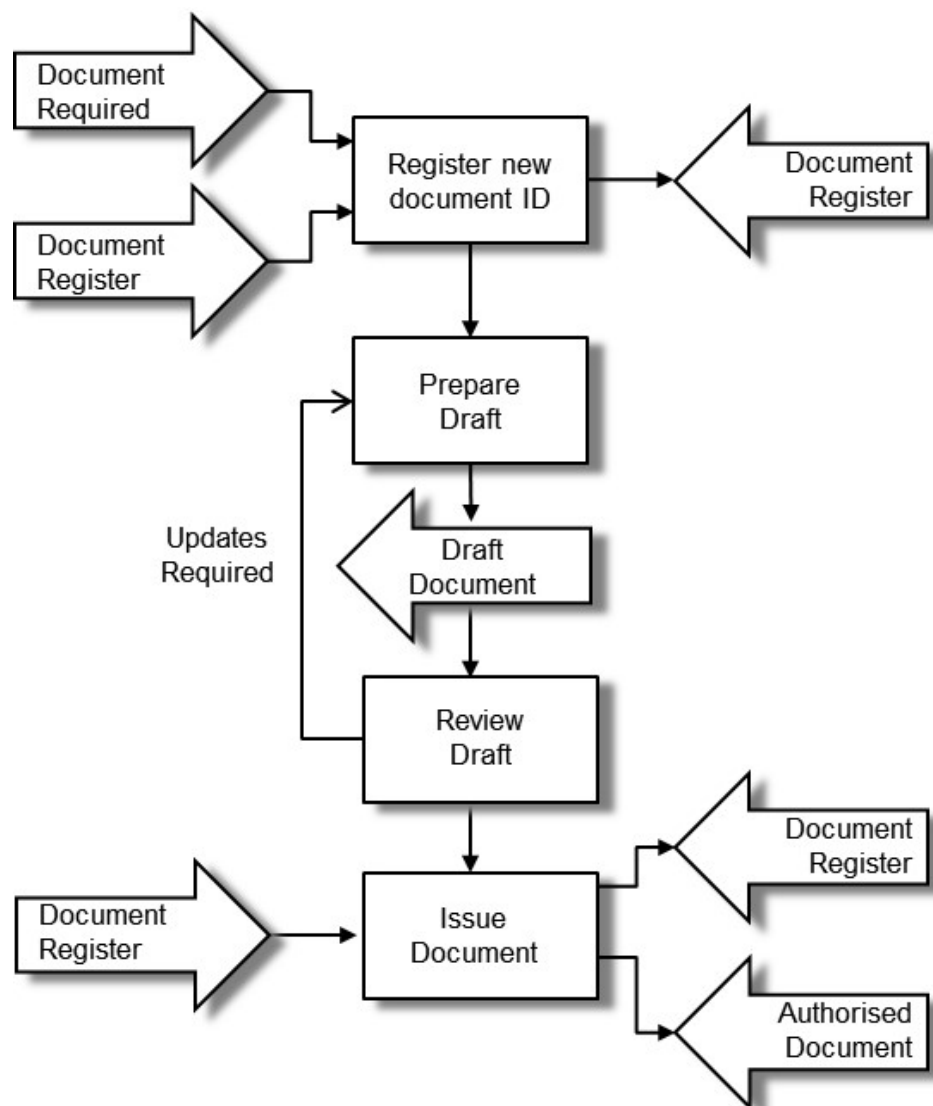
3.1 Responsibilities

All staff are responsible for ensuring documents are data are managed according to this policy and for making sure documents are data are not misused or released to unauthorised parties.

The Managing Director, or delegated authority, is responsible for authorising formally controlled documents for use within the Academy.

3.2 Document Control Process

Documents published as part of the school’s management systems are managed according to the following process.



A record of each controlled document is maintained in a document control register. The register includes a document reference ID, along with details of the author, the document title, it’s revision history and approval. The document control register also generates and automatic authentication code that is used to confirm authorisation of each document and traceability to it’s formal approval.



A new record is added to the document control register for each new document that is required or requested.

A draft document is then prepared by the author.

Draft documents must be clearly marked as draft must not be released or used within the school.

Draft documents are reviewed by at least one member of staff prior to issue. The draft document is annotated with any corrections or recommendations, as required.

Finalised documents are approved by the Managing Director or a delegated authority. The document is annotated with the authentication code generated by the document control register and is marked with a revision number, date of issue. The document is then printed and signed by the Managing Director. Signed copies are held on file.

The final document is marked as approved and is released in PDF format to minimise the risk of inadvertent or unauthorised changes being made.

3.3 **Data Backup and Recovery**

Data maintained on the school server is backed-up incrementally every day on removable backup media. A separate media drive is maintained for each working day (Monday-Friday). Backup drives are stored in a locked cabinet in the main office.

A further backup is taken at the end of every week, which is stored off-site in a locked and secure location.

Data lost through hard drive failure or corruption is recovered, in the first instance, through the most recent backup. However, particular care must be taken if loss has occurred through computer virus. In this case precautions are made to ensure that backup drives are not contaminated.

Previous or remote backups are only used for recovery where the most recent backup fails.

Remote backups will only be released for use in recovery with authorisation from the Managing Director.

3.4 **Storing Documents and Protective Markings**

All controlled documentation is marked with 'Robert Holme Academy and a copyright notice and year of issue in the footer.

The following classifications (below) are used to denote the controls applied to documents. The classification must be included in the footer of every controlled document

<b>Confidential</b>	Confidential documents include any with personal information or business critical data that is not available for general distribution.  Confidential documents must include a circulation list in the body of the document  The document must not be email, copied, printed or otherwise made available to anyone not included on the circulation list without prior authorisation from the Managing Director or delegated authority.  Printed copies of documents must be stored in a locked facility and must be destroyed after use.
<b>Private</b>	Private documents are for internal use only. They are available to all staff, but must not be email, copied or otherwise distributed to anyone outside the business.  Printed copies can be used but should be avoided wherever possible.
<b>RHA Proprietary</b>	Proprietary documents are available in the public domain and may be published on the academy website but remain the property of the school.