The James Hutton Institute

Records Management Policy

Prepared By: Evangelia Apostolakopoulou, Information Governance Officer & Thorntons Law LLP
Date: January 2020

Approved By: Hugh Darby, Director of Finance & Company Secretary
Date: 29 January 2020

Summary of Changes Since Previous Version:

See document control table at page 11.

Contents

1.0 Introduction

This Records Management Policy is designed to support the effective running of the James Hutton Institute (referred to in this Policy as "**Hutton**" or the "**Institute**") and aims to govern the management of all records produced or acquired by the Institute and its employees in the course of its business, and in all different media. Hutton recognises that its records are an asset, and effective management of its records supports its core functions whilst also contributing to effective overall management of the organisation. All records of Hutton must also be managed in compliance with relevant legislation and regulations, in furtherance of effective corporate governance and accountability.

There are legal and regulatory requirements for us to retain certain data, usually for a specified amount of time. We also retain data to help our business operate and to have information available when we need it. However, we do not need to retain all data indefinitely, and retaining data can expose us to risk as well as be a cost to our business. This Records Management Policy explains our requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal. Failure to comply with this Policy can expose us to fines and penalties, adverse publicity, difficulties in providing evidence when we need it and in running our business.

2.0 Legislative and Regulatory Framework

2.1 This Policy is based on the requirements as set out in Section 61, Code of Practice: Records Management, that accompanies the Freedom of Information (Scotland) Act 2002 and Hutton is committed to meeting its obligations under the legislation.

2.2 Hutton is also committed to ensuring that the management of its records is in compliance with the principles of the General Data Protection Regulation ((EU) 2016/679) ("**GDPR**") and the Data Protection Act 2018 ("**DPA**").

3.0 Audience

This Policy is for the attention of all Hutton Personnel. All of the records that Hutton Personnel create or administer in the process of Hutton business are official records of The James Hutton Institute, regardless of the media.

4.0 Purpose

This document provides the policy framework for the effective management of all the records of The James Hutton Institute.

5.0 Scope

5.1 This Policy applies to all records created, received or administered by Hutton Personnel in the course of their duties. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings. It applies to both Personal Data and non-Personal Data. In this Policy we refer to this information and these records collectively as "data".

5.2 This Policy covers data that is held by third parties on our behalf, for example cloud storage providers or offsite records storage.

5.3 Records which are created as a result of research are subject to the contractual record-keeping requirements of that research, whether it is externally or internally funded.

5.4 Records are defined as recorded information which provides evidence of some specific activity. Records can be in any media but will mainly comprise of paper or electronic formats.

5.5 Records Management is a means of systematically managing the creation, receipt, maintenance, use and disposal of records.

6.0 Guiding Principles

6.1 Through this Policy, and our data retention practices, we aim to comply with and meet the following commitments:

- We comply with legal and regulatory requirements to retain data.
- We comply with our data protection obligations.
- We handle, store and dispose of data responsibly and securely.
- We create and retain data where we need this to operate our business effectively, but we do not create or retain data without good business reason.
- We allocate appropriate resources, roles and responsibilities to data retention.
- We regularly remind employees of their data retention responsibilities.
- We regularly monitor and audit compliance with this Policy and update this Policy when required.

7.0 Personal Data protection principles

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);
(b) collected only for specified, explicit and legitimate purposes (Purpose Limitation);
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);

(d) accurate and where necessary kept up to date (Accuracy);
(e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);
(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality);
(g) not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and
(h) made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

7.1 Purpose Limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes. The Institute cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained, unless we have informed the Data Subject of the new purposes and they have consented where necessary.

7.2 Data Minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Hutton Personnel must only process Personal Data when their job duties require it. Hutton Personnel should not process Personal Data for any reason unrelated to their job duties. We must not collect excessive data. Hutton Personnel must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Institute's data retention guidelines.

7.3 Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

We must ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. The accuracy of any Personal Data at the point of collection and at regular intervals afterwards should be checked. We must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

Hutton will review Personal Data regularly to ensure that it is accurate, relevant and up to date. It must be corrected or deleted without delay when inaccurate.

7.4 Storage Limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. Hutton will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires that data to be kept for a minimum time.

Personal Data must not be kept in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it, including for the purpose of satisfying any legal, accounting or reporting requirements. We must take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require. This includes requiring third parties to delete that data where applicable. Data Subjects must also be informed of the period for which data is stored and how that period is determined in any applicable privacy notice.

7.5 Security of Personal Data

The Institute will ensure that Personal Data is not processed unlawfully, lost or damaged. Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of Personal Data. All Institute Personnel are responsible for protecting the Personal Data we hold. We must implement reasonable and appropriate security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. All Hutton Personnel employees must exercise particular care in protecting Special Category Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. Personal Data may only be transferred to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested. We must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it;
- Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed; and
- Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data. Should you have access to Personal Data during the course of your employment, you must also comply with this obligation.
If you believe you have lost any Personal Data in the course of your work, you must report it to your manager immediately. Failure to do so may result in disciplinary action up to and including dismissal without notice.

8.0 Types of data

8.1 **Formal or official records.** Certain data is more important to us. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business.

8.2 **Disposable information**. Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this Policy. Examples may include:

- Duplicates of originals that have not been annotated.
- Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record.
- Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of the Institute's and retained primarily for reference purposes.
- Spam and junk mail.

8.3 **Personal Data.** Both formal or official records and disposable information may contain Personal Data; that is, data that identifies living individuals. Data protection laws require us to retain Personal Data for no longer than is necessary for the purposes for which it is processed (principle of storage limitation).

8.4 **Confidential information belonging to others**. Any confidential information that an employee may have obtained from a source outside of Hutton, such as a previous employer, must not, so long as such information remains confidential, be disclosed to or used by us. Unsolicited confidential information submitted to us should be refused, returned to the sender where possible, and deleted, if received via the internet.

9.0 Storage, Back-up and Disposal of Data

9.1 **Storage.** Our data must be stored in a safe, secure, and accessible manner. Any documents and financial files that are essential to our business operations during an emergency must be duplicated and/or backed up at least once per week and maintained off site.

9.2 **Destruction**. Our Information Governance Officer is responsible for the continuing process of identifying the data that has met its required retention period and supervising its destruction. The destruction of confidential, financial, and employee-related hard copy data must be conducted by shredding if possible. Non-confidential data may be destroyed by recycling.

The destruction of data must stop immediately upon notification from the Information Governance Officer that preservation of documents for contemplated litigation is required (sometimes referred to as a litigation hold). This is because we may be involved in a legal claim or an official investigation (see next paragraph). Destruction may begin again once the Information Governance Officer lifts the requirement for preservation.

10.0 Special Circumstances

10.1 **Preservation of documents for contemplated litigation and other special situations.** We require all employees to comply fully with the procedures as provided in this Policy. All employees should note the following general exception to any stated destruction schedule: If you believe, or the Information Governance Officer informs you, that certain records are relevant to current litigation or contemplated litigation (that is, a dispute that could result in litigation), government investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those records, including emails and other electronic documents, until the Information Governance Officer determines those records are no longer needed. Preserving documents includes suspending any requirements in this policy and preserving the integrity of the electronic files or other format in which the records are kept.

10.2 If you believe this exception may apply, or have any questions regarding whether it may apply, please contact the Information Governance Officer.

10.3 In addition, you may be asked to suspend any routine data disposal procedures in connection with certain other types of events, such as our merger with another organisation or the replacement of our information technology systems.

11.0 Responsibilities

11.1 Hutton recognises and is committed to maintaining its records and record keeping systems in accordance with the legal and regulatory environment. Overall responsibility for this Policy lies with the Director of Finance & Company Secretary.

11.2 The Information Governance Officer is responsible for the development of good records management practice and promoting compliance with this Policy ensuring the efficient, appropriate and timely retrieval of information.

11.3 The Information Governance Officer is also responsible for the drafting of guidance relating to records management processes and procedures.

11.4 Individual employees must ensure that records for which they are responsible are accurate, maintained and disposed of appropriately.

12.0 Relationship with Existing Policies

This Policy is related to:
Policies and guidance on compliance with information legislation as found on the Hutton intranet on the Information Governance page.

13.0 Guidance

Guidance for staff on dealing with issues raised by this Policy is available from the Information Governance Officer, Evangelia Apostolakopoulou,
contact details as follows:
E-mail – Evangelia.Apostolakopoulou@hutton.ac.uk
Telephone – +44 (0)1224 395065
Extension – 5065

ANNEX – Definitions

Hutton Personnel: all employees, workers, contractors, agency workers, consultants, directors, members and any other individuals conducting business for or on behalf of the Institute including Honorary Fellows and Honorary Associates.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Criminal Convictions Data: means Personal Data relating to criminal convictions and offences and includes Personal Data relating to criminal allegations and proceedings.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Explicit Consent: Consent which requires a very clear and specific statement (that is, not just action).

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Document Control	
Title	**Records Management Policy**
Author/Creator	Information Governance Officer (IGO)/ Thorntons Law LLP
Owner	Information Governance Officer
Date Published/Approved	June 2017
Date of last update/approval	29 January 2020
Version	V.2.0
Date of Next Review	12 Months from published/approval date
Audience	All
Related Documents	Freedom of Information Policy, Data Protection Policy
Subject/Description	Following the Freedom of Information (Scotland) Act 2002 this policy outlines the obligations, rights and responsibilities of the Hutton and individuals as regards management of its records.
Group	Finance and Corporate Services
Department	Research Support

Summary of Changes to Document				
Date	Action by	Version Updated	New Version Number	Brief Description of amendments
29 January 2020	IGO/Thorntons	V.1.0	V.2.0	- Section 1.0: wording amendments, second paragraph added. - Section 2.0: updated information regarding legislative framework. - Section 3.0: spelling/wording corrections. - Section 5.0: Two (2) new paragraphs added. - Sections 6.0 – 8.0: previous Sections 6.0 – 8.0 replaced, their content currently released under numbering 11.0-13.0. New section 6.0 inserted, titled 'Guiding Principles'. New section 7.0, titled 'Personal Data Protection Principles'. New section 8.0, titled 'Types of Data'. - New section 9.0 inserted, titled 'Storage, Back-up and Disposal of Data'. - New section 10.0 inserted, titled 'Special Circumstances'. - New Section 11.0 added, replacing previous section 6.0 ('Responsibilities'). Minor spelling corrections. - New Section 12.0 added, replacing previous section 7.0 ('Relationship with Existing policies'). Minor spelling corrections. Deleted second paragraph, previously under 7.2. - New Section 13.0 added, replacing previous section 8.0 ('Guidance'). Minor spelling corrections. Updated Information Governance Officer contact name and contact details. - Annex – Definitions page added.