HP298 - DATA PROTECTION POLICY

Document ID:	HP298
Document title:	DATA PROTECTION POLICY
Dept.:	Projects and Contract Support
Document owner:	Information Governance Officer / Data Protection Officer
Details of review:	See table at Appendix 1 / Sharepoint document library on Connect

Contents

1. Overview 3
2. Definitions / glossary 3
3. About this Policy 5
4. Scope 5
5. Personal Data Protection Principles 6
6. Lawfulness, Fairness, Transparency 7
7. Consent 8
8. Transparency (Notifying Data Subjects) 8
9. Purpose Limitation 9
10. Data Minimisation 9
11. Accuracy 9
12. Storage Limitation 9
13. Protecting Personal Data 10
14. Reporting a Personal Data Breach 11
15. Transfer Limitation 11
16. Data Subject's Rights and Requests 12
17. Accountability 12
18. Record Keeping 13
19. Training and Audit 13
20. Privacy by Design and Data Protection Impact Assessment (DPIA) 13
21. Automated Processing (including Profiling) and Automated Decision-Making 14
22. Direct Marketing 15
23. Sharing Personal Data 15
24. Appendices 16
24.1 Appendix 1: Amendment and review 16
24.2 Appendix 2: Associated documents 16
24.3 Appendix 3: References 16

1. Overview

This Data Protection Policy ("Policy") applies to the James Hutton Institute ("we", "us", "our"), including Biomathematics & Statistics Scotland ("BioSS") and James Hutton Limited ("the Hutton Group") and its employees, workers, contractors, agency workers, consultants, directors, members and/or other individuals working or undertaking a role under or on behalf of Hutton Group ("you", "your").

The Policy sets out the principles and legal conditions which we must satisfy when obtaining, handling, processing, transporting or storing Personal Data in the course of our operations and activities, including research, marketing, student, consultant, volunteer and employee data. It is tailored to comply with the UK General Data Protection Regulation ("GDPR") and Data Protection Act 2018 and all other applicable data protection legislation ("Applicable Data Protection Law").

2. Definitions / glossary

Term / acronym	Definition
Automated Decision-Making (ADM)	when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The Applicable Data Protection Law prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.
Automated Processing	any form of Automated Processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.
BCR	Binding Corporate Rules
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, signifies agreement to the processing of Personal Data relating to them.
Criminal Conviction Data	means Personal Data relating to criminal convictions and offences and includes Personal Data relating to criminal allegations and proceedings.
Data Controller	the person or organisation that determines when, why and how to Process Personal Data. It is responsible for establishing practices and policies in line with the Applicable Data Protection Law
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.
Data Protection Impact Assessment (DPIA)	a tool and assessment used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design

Term / acronym	Definition
	and should be conducted for all major system or business change programs involving the processing of Personal Data
Data Protection Officer - DPO	a nominated person who is responsible for data protection issues within the organisation. Hutton's DPO can be contacted at DPO@hutton.ac.uk
Explicit Consent	consent which requires a very clear and specific statement (that is, not just an affirmative action).
Hutton colleagues	all employees, workers, contractors, agency workers, consultants, directors, members and others.
Information Commissioner or Information Commissioner's Office (ICO)	the supervisory data protection authority in the UK
IDTA	International Data Transfer Agreement
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 Category 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
Personal Data Breach	any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach
Privacy by Design	implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR
Privacy Notices	separate notices setting out information that may be provided to Data Subjects when the Hutton collects information about them
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.

Term / acronym	Definition
Special Category of Personal Data	information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.
UK GDPR	the version of EU General Data Protection Regulation (GDPR) retained in domestic law

3. About this Policy

This policy applies to all Personal Data we process regardless of the medium on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

You must read, understand and comply with this Policy when processing Personal Data on our behalf and attend/complete training on its requirements. This Policy sets out what we expect from you in order for the Hutton to comply with Applicable Data Protection Law. Your compliance with this Policy is mandatory. Related Policies and Procedures are available to help you interpret and act in accordance with this Policy. You must also comply with all such Related Policies and Procedures. Any breach of this Policy may result in disciplinary action.

This Policy (together with related Policies and Procedures) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the Data Protection Officer ("DPO"). This Policy does not override any domestic privacy laws and regulations in countries where the Hutton operates.

4. Scope

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Hutton is exposed to potential fines from the Information Commissioner's Office (ICO). The ICO has the power to impose a fine of up to 4% of our turnover or £17.5M, whichever is the greater; for failure to comply with the provisions of the Data Protection Laws. All departments are responsible for ensuring all Hutton Group colleagues comply with this Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

Please contact our DPO with any questions about the operation of this Policy or Applicable Data Protection Law or if you have any concerns that this Policy is not being or has not been followed. In particular, you must always contact our DPO in the following circumstances:

- if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Hutton) (*see Section 6 below*);
- if you need to rely on Consent and/or need to capture Explicit Consent *(see Section 7 below)*;
- if you need to draft Privacy Notices (*see Section 8 below*);

- if you are unsure about the retention period for the Personal Data being processed (*see Section 12 below)*;
- if you are unsure about what security or other measures you need to implement to protect Personal Data (*see Section 13 below)*;
- if there has been a Personal Data Breach (*see Section 14 below)*;
- if you are unsure on what basis to transfer Personal Data outside the UK (*see Section 15 below*);
- if you need any assistance dealing with any rights invoked by a Data Subject (*see Section 16 below*);
- whenever you are engaging in a significant new, or change in, processing activity which is likely to require a DPIA *(see Section 20 below)* or plan to use Personal Data for purposes others than what it was collected for;
- if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making *(see Section 21 below)*;
- if you need help complying with applicable law when carrying out direct marketing activities *(see Section 22 below)*; or
- if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) *(see Section 23 below)*.

Hutton's DPO should be able to operate without conflict. In the event that there is a conflict of interest, please refer to our DPO Conflicts of Interests Procedure for further guidance.

5. Personal Data Protection Principles

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

- Processed lawfully, fairly and in a transparent manner *(Lawfulness, Fairness and Transparency).*
- Collected only for specified, explicit and legitimate purposes (Purpose Limitation).
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed *(Data Minimisation).*
- Accurate and where necessary kept up to date *(Accuracy).*
- 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).*
- 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).*
- Not transferred to another country without appropriate safeguards being in place *(Transfer Limitation).*
- Made available to Data Subjects and Data Subjects allowed 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).*

6. Lawfulness, Fairness, Transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The UK GDPR allows processing for specific purposes, some of which are set out below:

- the Data Subject has given his or her Consent;
- the processing is necessary for the performance of a contract with the Data Subject;
- to meet our legal compliance obligations;
- to protect the Data Subject's vital interests;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- to pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we Process Personal Data for legitimate interests need to be set out in applicable Privacy Notices and we need to undertake a Legitimate Interest Test. Please see our Legitimate Interests Test and Guidance Procedure and Assessment for further guidance.

Where we Process Special Category of Personal Data, we can only do so where we can meet one basis in paragraph 7.3 above and one basis set out in Clause 9 of UK GDPR, most of which are set out below:

- Explicit consent, except where domestic law provides that we cannot rely on consent;
- necessary for purposes of carrying out our obligations and exercising our rights as an employer or to allow the data subject to carry out their obligations or exercise their right as an employee;
- to protect the Data Subject's vital interests;
- Processing relates to Personal Data which are manifestly made public by the Data Subject;
- Processing is necessary for the establishment, exercise or defence of legal claims;
- substantial public interest;
- preventive or occupational medicine, for the assessment of the working capacity of the employee on the basis of domestic law or pursuant to contract with a health professional;
- necessary for reasons of public interest in the area of public health; or
- necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Art 89(1) (as supplemented by Section 19 of the 2018 Act) based on domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the Data Subject.
- For further guidance on how we process and protect Special Category Data and Criminal Convictions Data, please see our Appropriate Policy Document.

7. Consent

A Data Controller must only Process Personal Data on the basis of one or more of the lawful bases set out in the UK GDPR, which include Consent.

A Data Subject consents to processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw Consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Unless we can rely on another legal basis of processing, Explicit Consent is usually required for processing Special Category of Personal Data, for Automated Decision-Making, for processing of Criminal Convictions Data and for cross border data transfers. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Special Category of Personal Data. Where Explicit Consent is required, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent. You will need to evidence Consent captured and keep records of all Consents so that the Hutton can demonstrate compliance with Consent requirements.

8. Transparency (Notifying Data Subjects)

The UK GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the UK GDPR including the identity of the Data Controller and DPO, how and why we will use, process, disclose, protect and retain that Personal Data. The above information will be normally provided via a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.
When Personal Data is collected indirectly (for example, from a third party or publicly available source), you must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed processing of that Personal Data.

Please refer to our Privacy Notice Procedure for further guidance on information you need to provide to Data Subjects when collecting Personal Data.

9. 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.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have consented where necessary.

10. Data Minimisation

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

You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Hutton's data retention guidelines.

11. Accuracy

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

You will 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. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

12. 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.
You must not keep Personal Data 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.

The 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 such data to be kept for a minimum time. You must comply with the Hutton's guidelines on Data Retention.

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Hutton's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

13. Protecting Personal Data

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 operations, 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. You are responsible for protecting the Personal Data we hold. You 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. You must exercise particular care in protecting Special Category of Personal Data from loss and unauthorised access, use or disclosure.

Examples of security measures that you can implement to protect Personal Data include, but are not limited to:

- Using strong passwords to protect your device. Do not write your passwords on devices or paper and do not share your password.
- Do not leave your devices unattended in public spaces.
- Lock your devices before stepping away from it, whether you are working from the office or at home.
- Do not save or store company documentation locally on your devices.
- Do not share contents or details of Hutton's documentation with anyone who is not authorised to see it.
- Store and dispose of physical documents safely and appropriately.

For further information on data security, please refer to the organisation's ITS Policies and Procedures.

Also, the ICO's guidance on data security can be found here: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/

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. You may only transfer Personal Data 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.

You 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.
- 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 UK GDPR and relevant standards to protect Personal Data.

14. Reporting a Personal Data Breach

The UK GDPR requires Data Controllers to notify any Personal Data Breach to the Information Commissioner Office and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so. Please read the Personal Data Breach Procedure (HP082).

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact our Data Protection Officer. You should preserve all evidence relating to the potential Personal Data Breach. Please refer to our Personal Data Breach Procedure (HP082) for further information on what you should do in these circumstances.

15. Transfer Limitation

The UK GDPR restricts data transfers to countries outside the UK in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer Personal Data originating in the UK across borders when you transmit, send, view or access that data in or to a different country.

You may only transfer Personal Data outside the UK if one of the following conditions applies:

- The UK has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;
- Appropriate safeguards are in place such as Binding Corporate Rules (BCR"), addendum to the standard contractual clauses or International Data Transfer Agreement ("IDTA") approved for use in the UK, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;
- The Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
- The transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to

establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

Please speak with our DPO before transferring any Personal Data outside of the UK.

16. Data Subject's Rights and Requests

Data Subjects have rights when it comes to how we handle their Personal Data. Please read over and comply with the Data Subjects Rights Procedure. These include rights to:

- withdraw Consent to processing at any time;
- receive certain information about the Data Controller's processing activities;
- request access to their Personal Data that we hold;
- prevent our use of their Personal Data for direct marketing purposes;
- ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
- restrict processing in specific circumstances;
- challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which Personal Data is transferred outside of the UK;
- object to decisions based solely on Automated Processing, including profiling ("Automated Decision Making", "ADM");
- prevent processing that is likely to cause damage or distress to the Data Subject or anyone else;
- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the supervisory authority; and
- in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation). Please refer to the Proof of Data Subject Identity template.

You must immediately forward any Data Subject Request you receive to our Information Governance Officer/Data Protection Officer.

17. Accountability

The Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

The Hutton must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

- appointing an executive accountable for data privacy;

- implementing Privacy by Design when processing Personal Data and completing DPIAs where processing presents a high risk to rights and freedoms of Data Subjects;
- integrating data protection into internal documents including this Policy, Related Policies and Procedures, Privacy Guidelines, and Privacy Notices;
- regularly training employees on the GDPR, this Policy, Related Policies and Procedures and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Hutton Group must maintain a record of training attendance by Hutton employees; and
- regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

18. Record Keeping

The UK GDPR requires us to keep full and accurate records of all our data processing activities. You must keep and maintain accurate corporate records reflecting our processing including Records of Data Subjects' Consents and procedures for obtaining Consents.

These records should include, at a minimum, the name and contact details of the Data Controller, clear descriptions of the Personal Data types, Data Subject types, Processing Activities, Processing Purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

19. Training and Audit

We are required to ensure all employees have undergone adequate training to enable them to comply with data Privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory Data Privacy related training and ensure your team undergo similar mandatory training.

ITS team shall review all the systems and processes under your control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

20. Privacy by Design and Data Protection Impact Assessment (DPIA)

We are required to implement Privacy by Design measures when processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data Privacy principles.

We have a DPIA Procedure – HP081 which should be read and complied with when implementing major system or business change programs involving the processing of Personal Data.

However essentially, you must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account: the cost of implementation, the nature, scope, context and purposes of the processing; and the risks of varying likelihood and severity to the rights and freedoms of the Data Subjects posed by the processing.

Examples of when you should conduct a DPIA include but are not limited to:

- Use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- Automated Processing including profiling and ADM;
- Large scale Processing of Special Category of Personal Data or Criminal Convictions Data; and
- Large scale, systematic monitoring of a publicly accessible area.

21. Automated Processing (including Profiling) and Automated Decision-Making

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

- a Data Subject has explicitly consented;
- the processing is authorised by law; or
- the processing is necessary for the performance of or entering into a contract.

If certain types of Special Category of Personal Data or Criminal Convictions Data are being processed, then grounds (b) or (c) will not be allowed but such Special Category of Personal Data and Criminal Convictions Data can be processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

A DPIA must be carried out before any Automated Processing (including profiling), or ADM activities are undertaken.

22. Direct Marketing

We will engage in marketing activities to promote our services, ideals or aims. We would recommend that the Marketing Team consider these closely when they are engaging in any new marketing activities. We are subject to certain rules and privacy laws when marketing to our customers.

For example, a Data Subject's prior consent is usually required for electronic direct marketing (for example, sending out marketing communications via email regarding out services, ideals or aims.). The limited exception for existing customers known as "soft opt in" allows some organisations to send marketing texts or emails if they have obtained contact details in the course of the provision of services to that person, they are marketing similar services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message. Typically, we can rely on legitimate interest and therefore not obtain consent if we market to third party organisations or employees of third-party organisations provided they are receiving the message as a representative of their employer.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

23. Sharing Personal Data

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place. Please refer to our Third-Party Data Sharing Procedure for detailed guidance on how to ensure compliance when sharing personal data.

You may only share the Personal Data we hold with another employee, agent or representative of our group if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers if:

- they have a need to know the information for the purposes of providing the contracted services;
- sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable cross-border transfer restrictions; and
- a fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

24. Appendices

24.1 Appendix 1: Amendment and review

Version	Amendment and review details
1	Initial publication NOTES: • This Policy supersedes the previous 'GDPR Policy' (published May 2018) • This Policy is subject to organizational document review timeframes. From time to time we may need to make edits to this Policy to reflect changes in data protection legislation and how we process Personal Data. Any significant changes to the content of this Policy will be made in consultation with the Union or appropriate internal Body/Group before the updated version is published and implemented.
2	Paragraph number amendment

24.2 Appendix 2: Associated documents

All Hutton Group's policies, operating procedures or processes related to this Policy and designed to protect Personal Data, including without limitation:

Document ID	Document title
HP293	Appropriate Policy Document
HP294	Data Sharing with Third Party Procedure
HP295	Data Subjects Rights Procedure
HP296	Legitimate Interest Procedure and Assessment
HP297	Privacy Notice Procedure
HP081	DPIA Procedure
HP082	Personal Data Breach Procedure
(Currently Under development)	DPO Conflicts of Interest Procedure

24.3 Appendix 3: References

Document title
Data Protection Act 2018
ICO's guidance on data security
UK GDPR