James Hutton Group

General Data Protection Regulation Personal Data Breach Policy and Guide

Prepared By: Information Governance Officer
Date: April 2018

Approved By: Data Protection Officer
Date: 9 May 2018

Summary of Changes Since Previous Version:
New Policy.

CONTENTS

Introduction

This document applies to the employees, staff, workers and/or other individuals working or undertaking a role under or on behalf of the James Hutton Group which consists of The James Hutton Institute ("Hutton") including Biomathematics & Statistics Scotland ("BioSS") and James Hutton Limited ("JHL"). Hutton is a data controller in respect of all personal data it processes and JHL is a data controller in respect of the personal data it processes. When the terms 'we', 'us' or 'our' are used it should be read as referring to the James Hutton Group, unless otherwise specified.

The James Hutton Group (is responsible for the security, integrity and confidentiality of all the data it holds. The General Data Protection Regulation (GDPR) not only requires that personal data is kept safe and secure but it also introduces a new requirement for all UK organisations, including the Hutton Group, to report certain types of personal data breaches to the Information Commissioner's Office (ICO).

When notifying the ICO of a personal data breach, this must be done without delay where feasible and no later than 72 hours of becoming aware of the breach. In the event that the data breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, organisations must also inform those individuals affected without undue delay.

Organisations, such as the Hutton Group, whom act as data controllers are encouraged to plan in advance and put in place processes to be able to detect and promptly contain a breach and to assess the risk it poses to individuals. The GDPR also requires the implementation of robust breach detection, investigation and internal reporting procedures that will facilitate decision-making about whether or not the ICO and the affected individual(s) need to be notified. Under the GDPR, records of any personal data breaches must be maintained, regardless of whether or not you are required to notify that the breach has taken place.

All staff have a responsibility for the information that they generate, manage, transmit and use in line with the GDPR. However it is also their contractual duty to secure personal and confidential data at all times. Any person who knows or suspects that a breach of data security has occurred should report the breach immediately in accordance with Data Breach Policy.

It is vital that the Hutton Group and all Hutton Group staff take prompt action in the event of any actual, potential or suspected breaches of data security or confidentiality to avoid the risk of harm to stakeholders or employees, damage to operational business and severe financial, legal and reputational costs to the Hutton Group.

Purpose

The purpose of this policy and guide is to provide a distinctive framework for the reporting and managing of any personal data breaches affecting confidential, personal or special category data (defined below) held by the Hutton Group. This policy and guide is a supplement to the Hutton Group's General Data Protection Regulation (GDPR) Policy which iterates Hutton Group's commitment to protecting the privacy rights of data subjects in accordance with the GDPR.

If the Hutton Group fails to notify either the ICO or where appropriate, data subjects affected by the data breach or both, Hutton Group

could have to pay an administrative fine. The value of this can be up to 10,000,000 EUR or up to 2% of the total worldwide annual turnover. It is also important to bear in mind that in some cases, the failure to notify a breach could reveal either an absence of existing security measures or an inadequacy of the existing security measures. In that case, the ICO will also have the possibility to issue sanctions for failure to notify or communicate the breach on the one hand, and absence of (adequate) security measures on the other hand, as they are two separate infringements.

Accordingly, all staff members of the Hutton Group have an important role to play when following the data security breach procedure, enabling Hutton Group to comply with GDPR and avoid hefty fines.

What is a personal data breach?

A personal data breach is 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed' (Art 4 of GDPR). One of the consequences of a personal data breach would be the Hutton Group being unable to ensure compliance with the confidentiality and integrity principle as outlined in Article 5 of the GDPR. Breaches can be categorised based on the following information security principles;

- Confidentiality breach – where there is an unauthorised or an accidental disclosure of, or access to, personal data.
- Integrity breach – where there is an unauthorised or an accidental alteration of personal data.
- Availability breach – where there is an accidental or an unauthorised loss of access to or, destruction of, personal data.
- Loss or destruction breach – where personal data is lost or stolen.

It should be noted that, depending on the circumstances, a breach can concern confidentiality, availability and integrity of personal data at the same time, as well as any combination of these. Personal data security breaches which would fall into the above categories would include the following for example

- disclosing confidential data to unauthorised individuals;
- loss or theft of portable devices containing personal or special category personal data e.g. laptops, PCs, mobile phones, USB, disks, etc.;
- loss or theft of paper records;
- inappropriate access controls on electronic folders/files/drives which allows unauthorised access/use of personal data;
- suspected breach of the Hutton Group's IT Security and Acceptable Use policies;
- attempts to gain unauthorised access to computer systems e.g. hacking;
- records altered or deleted without appropriate consent/authorisation from the data subject;
- viruses or other attacks on ITS equipment, systems or networks;
- breaches of physical security e.g. breaking into secure rooms or filing cabinets where confidential personal data is stored;
- confidential personal data left unlocked in accessible areas;
- unsecure disposal of confidential paper waste;
- leaving PCs unattended when logged on to a user account without locking the screen to stop others

accessing information;

- disclosing passwords to colleagues or others who could then gain unauthorised access to data;
- publication of confidential personal data onto the Hutton, JHL or BioSS websites or internet in error;
- misdirected e-mails containing personal, confidential or special category data.

What types of data does this policy and guide apply to?

This policy and guide applies to:

- all personal data created or received by the Hutton Group in any format (including paper records), whether used in the workplace, stored on portable devices and media, transported from the workplace physically or electronically or accessed remotely;
- personal data held on all Hutton Group IT systems managed centrally by ITS, and locally by individual departments/groups; and
- any other IT systems on which Hutton Group's data is held or processed.

Who is responsible for managing personal data security breaches?

Personal data security breaches are managed by Hutton's Data Protection Officer (DPO) in conjunction with the Head of ITS and the Director of Finance and Company Secretary where appropriate.

In emergency data security breach situations Hutton's Executive will manage the incident under the direction of the DPO.

Procedure for reporting data security breaches.

In the event of a breach of data security occurring within the Hutton Group, it is vital to ensure that it is dealt with immediately and appropriately to minimise the impact of the breach and prevent a recurrence.

If a personal data breach or potential or suspected personal data breach has been reported to you and/or you otherwise become aware of a personal data breach please report this immediately to the Data Protection Officer by e-mail to DPO@hutton.ac.uk or by telephone on 01382 346814 or 07525 592176. The attached Data Security Breach Report form should also be completed and e-mailed to the DPO at DPO@hutton.ac.uk as soon as possible after the initial reporting.

This report should record all relevant details of the incident and should be communicated to all relevant staff on a strictly confidential basis to ensure that a prompt and appropriate action is taken to resolve the breach incident.

- The DPO must then :Notify the Head of ITS and the Director of Finance and Company Secretary of the breach event;
- As stated in Article 33 of the GDPR if the breach is likely to result in a risk to individuals report the incident within 72 hours to the ICO;
- If the breach will impact and result in a risk to individuals the DPO must also take steps to notify the

individuals affected;

- If the DPO decides that the breach does not require to be reported to the ICO it should still be documented as a breach with an explanation justifying why it did not need to be reported to the ICO.

Procedure for managing personal data security breaches.

When managing a personal data breach the following five steps should be followed:

1. Identification and initial assessment.
2. Containment and recovery.
3. Risk assessment.
4. Notification.
5. Evaluation and response.

1. Identification and initial assessment.

As soon as a personal data breach has occurred it must be reported immediately to the DPO. The DPO will then liaise with the Head of ITS and the Director of Finance and Company Secretary. The individual reporting the breach should also complete the attached Data Security Breach Report Form and e-mail it to the DPO without delay. Part 1 of the report form will assist the DPO in conducting the initial assessment of the breach in order to establish:

- if a personal data security breach has in fact taken place;
- if a personal data security breach has occurred, what data has been involved/affected;
- the cause of the breach;
- the extent of the breach and how many individuals have been affected;
- the level of harm/risk to the individuals affected by the breach;
- how the breach can be contained.

After the initial assessment of the breach the DPO will, in consultation with the Director of Finance and Company Secretary and the Head of ITS, liaise with the appropriate head of department/science group leader to carry out a full investigation of the breach event. Should the breach be significant, the DPO will also consider whether or not to establish a Breach Management Team made up of appropriate Hutton Group staff and/or third parties e.g. insurers or lawyers to assist with the investigation. All records relating to the investigation will be retained by the DPO.

The DPO will use the undernoted table to determine the severity of the incident and this will be recorded on part 2 of the Data Security Breach Report Form. Depending on the level of the breach ,the DPO will decide whether the incident can be managed/controlled at a local level or if it has to be escalated to the Hutton Executive team. If the DPO deems the severity of the breach to be level 3 or above then the Executive will be actively involved in the management of the event.

Breach Rating	0 MINOR	1 LOW	2 HIGH	3 SERIOUS	4 SERIOUS	5 SERIOUS	6 ICO PENALTIES
Hutton Group's Reputation	No significant impact on any individual/group of individuals. Media interest very unlikely.	Damage to an individual's reputation or possible misuse of their personal data. Media interest possible.	Damage to a Hutton Group department/science group's reputation. Media interest possible but it may not penetrate the public domain.	Damage to more than one Hutton Group department/science group's reputation. Possible key local media coverage	Damage to Hutton Group's reputation. Breach impacts on >20 but < 50 data subjects. Local media coverage of breach.	Damage to Hutton Group's reputation. Breach impacts on >50 data subjects. National media coverage.	Breach will carry monetary penalty from ICO.
Data Subjects Potentially Affected	**MINOR** breach of confidentiality. Only a single data subject affected.	Breach is potentially serious but <10 data subjects affected and/or risk assessed as **LOW** e.g. files were encrypted.	Potential serious breach & risk assessed as **HIGH** e.g. unencrypted special category records lost. Breach impacts on <50 data subjects.	**SERIOUS** breach of confidentiality e.g. up to 100 data subjects affected e.g. loss of personal data relating to redundancies where data subjects clearly identifiable.	**SERIOUS** breach with either particular sensitivity /special category personal data e.g. medical records or up to 1000 data subjects affected.	**SERIOUS** breach with potential for identity theft and/or over 1000 data subjects affected.	**ICO PENALTIES.** Restitution to affected data subjects. Other liabilities such as systems updates/new software. Additional systems/records Security. Legal Costs

2. Containment and recovery.

Once it has been established that a data breach has occurred the Hutton Group must take immediate and appropriate action to limit the breach. Accordingly, the DPO with assistance from the Head of ITS will:

- Establish who within the Hutton Group needs to be made aware of the breach and advise them what needs to be done to contain the situation;
- Establish if anything can be done to recover any lost data and limit the damage of the breach e.g. physical recovery of the records, restoration of the data via back-up tapes;
- Establish if it is appropriate to notify affected data subjects immediately i.e. where the risk/harm to the data subjects has been deemed as high/serious.
- If appropriate, inform the Police in cases which involve data theft or other criminal activity relating to personal data.

3. Risk Assessment.

Although the GDPR introduces the obligation to notify a breach, it is not a requirement to do so in all circumstances. Upon becoming aware of a breach, it is vitally important that the Hutton Group carries out a risk assessment of the breach and seeks to contain the incident.

In assessing the risk arising from a personal data breach, the DPO along with all relevant members of Hutton Group staff, are required to consider the potential adverse impact on data subjects i.e. what is the likelihood of actual harm to the affected data subjects is and how serious or substantial is the impact likely to be. The information completed at Section 1 of the Data Security Breach Report Form will assist with this part of the risk assessment.

The DPO, along with the relevant Hutton Group head of department/science group leader/manager of the area where the breach occurred, will review the breach report in order to assess the risks and consequences of the breach for both the data subjects involved and for the Hutton Group.

Risks for Data Subjects:

- the risk for the affected data subjects i.e. adverse consequences of the breach and how substantial/serious it is;
- the likelihood of it recurring.

Risks for the Hutton Group:

- strategic and operational;
- compliance and legal;
- Financial;
- business continuity;
- reputational damage.

Consideration must also be given to the following:

- What type of personal data has been involved in the breach i.e. is it special category personal data?;
- Was the data protected in any way? e.g. encryption which would make it less accessible;
- What has actually happened to the data in question?;
- If it has been stolen, could the type of data be used for other purposes which would be of significant harm to the data subjects involved?;
- How many data subjects have been affected by the personal data breach? The assumption should not necessarily be that the risks are greater where large amounts of data have been lost. However, this is a vital factor to be considered and scrutinised;
- Whose personal data is the subject of the breach i.e. is it Hutton Group staff, stakeholders, customers? This will, to some extent, determine the level of risk posed by the breach and will also direct the actions in mitigating the risks;

- What harm could come to the data subjects affected by the breach? Are there potential risks to their physical safety, financial security or reputation or a combination of these factors?

Personal data breaches that are likely to result in high risk to the rights and freedoms of individuals would be circumstances where the breach may lead to physical, material or non-material damage for the individuals whose data have been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related to security measures, such damage should be considered likely to occur.

The DPO should determine, where appropriate, what remedial action should be taken on the basis of the breach report to mitigate the impact of the breach and also to ensure that the breach does not recur.

The DPO will prepare an incident report which will set out, where applicable, the following:

- a summary of the security breach;
- the individuals involved in the security breach (such as employees, contractors, external clients);
- details of the information, Hutton Group IT systems, equipment or devices involved in the security breach and any information lost or compromised as a result of the incident;
- how the breach occurred;
- actions taken to resolve the breach;
- impact of the security breach;
- unrealised, potential consequences of the security breach;
- possible courses of action to prevent a repetition of the security breach;
- side effects, if any, of those courses of action; and
- recommendations for future actions and improvements in data protection as relevant to the breach incident.

This report will then be provided to Hutton's Board, the Chief Executive and the head of department/science group leader/manager whose department was impacted by the breach. All relevant risk registers must be updated in respect of the personal data breach. Significant risks will be reported to both the Board and Hutton Group's Audit and Finance Committee with matters addressed appropriately in line with Hutton Group's Risk Management Policy.

4. Notification.

After taking the above into consideration, the DPO and the other relevant members of Hutton Group staff involved in the management of the breach, will determine whether or not it is necessary to notify the breach outside of the Hutton Group. Those that may need to be notified are:

- the data subjects affected by the breach
- the stakeholders/external funding organisations
- the Information Commissioner's Office (if the breach poses a risk to data subject/s)
- the Police

- the press/media
- Hutton Group's solicitors
- Hutton Group's insurers

If the breach may cause a risk to individuals, the breach must be reported to the ICO. When notifying the ICO, as a minimum, the notification must include:

- a description of how and when the personal data breach occurred;
- what personal data was involved;
- who are the data subject involved;
- approximate number of personal data records concerned;
- the likely consequences of the personal data breach; and
- what action has been taken to respond to/resolve the risks posed by the breach.

Subject to certain exemptions, if the personal data breach causes, or is likely to cause, a high risk to the data subjects, it may be necessary to inform the data subjects. If it is deemed necessary to notify the data subject(s) of the breach, the DPO must provide the data subjects in plain and clear language information on :

- the name and contact details of Hutton's DPO or other point of contact;
- the likely consequences of the personal data breach;
- the measures taken or proposed to be taken by the Hutton Group to address the personal data breach, including where appropriate, measures to mitigate its possible adverse effects.

The DPO must also decide on the most appropriate method of notification of the breach based on the following:

- Are there a large number of data subjects involved?;
- Does the breach involve special category personal data?;
- Is it necessary to write to each individual affected?;
- Should legal advice be sought on the wording of the notification?

The DPO must also ensure that the notification has a clear purpose e.g. that it enables the affected data subjects to take the necessary steps to protect themselves e.g. through cancelling bank cards, changing passwords etc., to allow regulatory bodies to perform their functions, provide advice and deal with any complaints. The focus of any breach response plan should be on protecting individuals and their personal data.

Timeframes

If the Hutton Group decides that it should (or if the ICO determines that the Hutton Group must) inform the data subjects, this must be done without undue delay.

Where a decision is taken that it is necessary to notify the ICO, this must be done by the DPO within 72 hours from the point that the Hutton Group became aware of the incident. The Hutton Group will be

regarded as having become “aware” when the Hutton Group has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. This will depend on the circumstances of the specific breach. In some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish whether or not the personal data has been compromised.

Where precise information is not available (e.g. the exact number of data subjects affected) this should not be a barrier to timely breach notification. The GDPR allows for approximations to be made in the number of individuals affected and the number of personal data records concerned as it recognises that controllers may not always have all details of the incident available during this initial period.

It is more likely this will be the case for more complex breaches, such as some cyber security incidents where, for example, an in-depth forensic investigation may be necessary to fully establish the nature of the breach and the extent to which personal data have been compromised.

Consequently, in some cases, the Hutton Group will have to do more investigation and follow-up with additional information at a later point. This is permissible as long as the Hutton Group provides reasoning for the delay. It should be noted that there is no penalty for reporting an incident that ultimately transpires to not be a breach.

The focus instead when reporting a breach should be directed towards addressing the adverse effects of the breach rather than providing precise figures of those affected. Thus, when it has become clear that there has been a breach, but the extent of it is not yet known, a notification in phases is a safe way to meet the notification obligations.

5. Evaluation and response.

Subsequent to a personal data breach the DPO, in consultation with the relevant members of Hutton Group staff, will conduct a review to ensure that the steps taken during the incident were appropriate and to identify any areas for improvement.

The DPO will report all data breaches to the Hutton Board and the Executive Team, also maintaining a central record of all breach occurrences. However, for any serious breaches the DPO will conduct a review and provide a detailed report to the Hutton Board and the Executive Team stating:

- the action which needs to be taken to reduce the risk of future breaches to minimise their impact;
- whether any policies, procedures or reporting lines require improvement to increase the effectiveness of response to the breach;
- if there are any faults or weak points in security controls which need to be tightened up;
- staff awareness/training issues which would prevent recurrence of the breach;
- additional investment in resources/infrastructure to reduce exposure to breach and relating cost implications.

It is important to keep in mind that, regardless of whether or not a breach needs to be notified to the ICO,

under Article 33(5) of the GDPR, the Hutton Group must keep documentation of all breaches comprising the facts relating to the personal data breach, its effects and consequences and the remedial action that was taken. The Hutton Group will also record its reasoning for the decisions taken in response to a breach, in particular, if the breach has not been notified, a justification for that decision made. This documentation will enable the Hutton Group to verify its compliance with the Regulation, as these records can be requested by the ICO. This is linked to the important accountability principle of the GDPR, contained in Article 5(2). Controllers, like Hutton and JHL, are encouraged to establish an internal register of breaches, regardless of whether they are required to notify or not. If the Hutton Group fails to adequately document this process, there will be financial penalties in accordance with Article 83.

Related Hutton Group Policies and Procedures.

This policy and guide supports the following Hutton Group policies and procedures:

- General Data Protection Regulation Policy
- Records Management Policy
- ITS Cyber Security Policy

Further Assistance and Advice

For any further assistance and advice about this policy and about any data protection matters please contact the Data Protection Officer:

By e-mail on DPO@hutton.ac.uk
By Telephone on 01382 346814

The ICO have also introduced a helpline to answer any queries that persons may have regarding a potential personal data security breach:

Tel: 0303 123 1113

Appendix 1 – Personal Data Security Breach Report Form

Please act promptly to report any data security breaches. If you discover a data security breach, please notify your Head of Department/Science Group immediately. Heads of Department/Science Group should complete Section 1 of this form and email it to the Data Protection Officer at DPO@hutton.ac.uk as soon as practically possible. The Head of Department/Science Group should also call the DPO on 01382 346814 and/or on 07525592176 to ensure the DPO has received the email.

Section 1: Notification of Data Security Breach	To be completed by Head of Dept/Science Group of person reporting incident
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If,so please provide details:	
Brief description of any action taken at the time of discovery:	

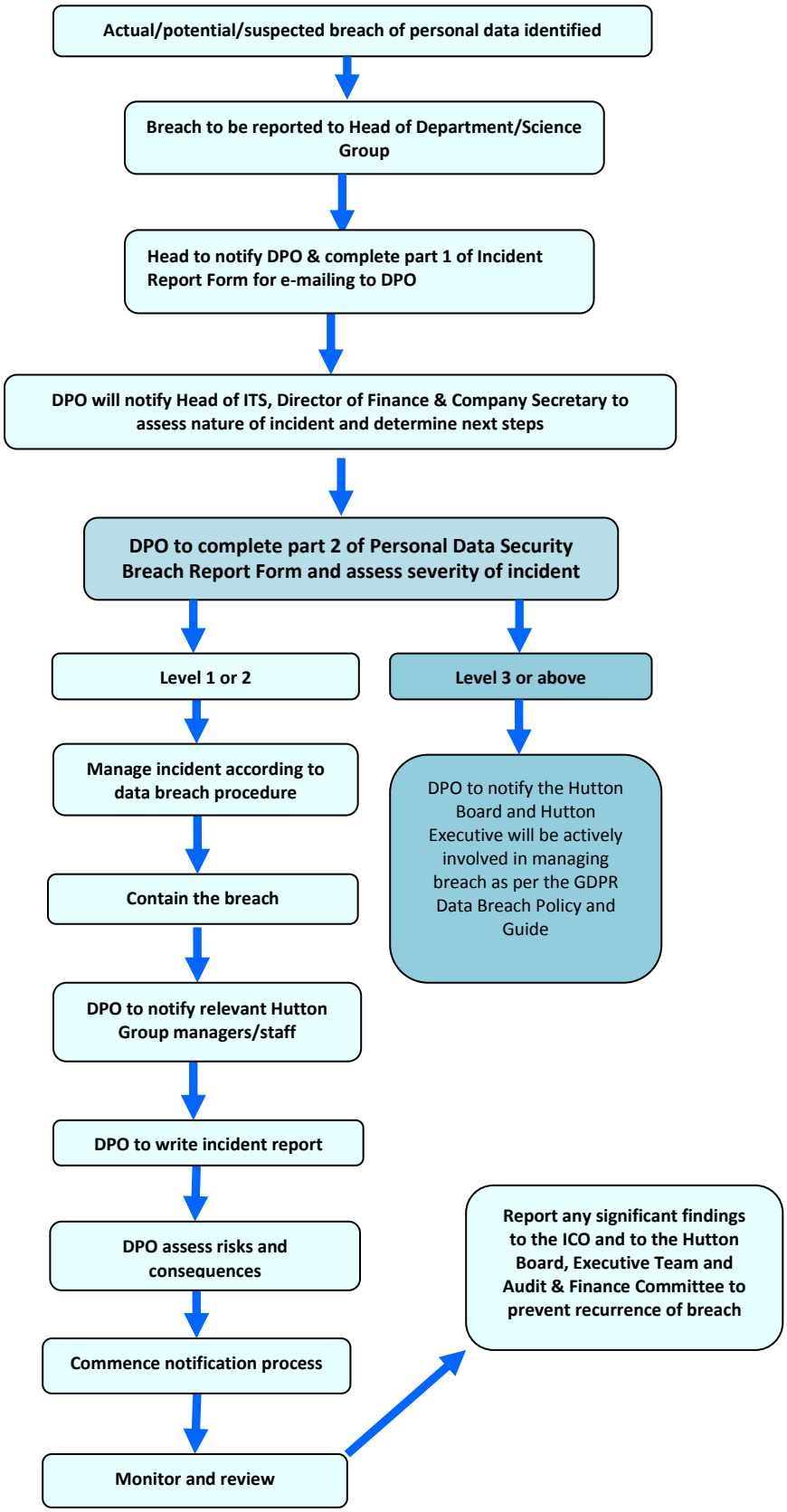
For Hutton DPO use	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	To be completed by DPO in consultation with the Head of Dept/Science Group affected by the breach
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the firm or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data ○ **Special Category Personal Data** (as defined in the GDPR) relating to a living, identifiable individual's •race; •ethnic origin; •politics; •religion; •trade union membership; •genetics; •biometrics (where used for ID purposes); •health; •sex life; or •sexual orientation.	
○ Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers, such as National Insurance Number and copies of passports and visas;	

○ Personal information relating to vulnerable adults and children;	
○ Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
○ Security information that would compromise the safety of individuals if disclosed.	
Category of incident (0-6):	
Reported to Incident Manager on:	
If level 3 or above, date escalated by DPO the Hutton Executive Team	

Section 3: Action taken	**To be completed by DPO**
Incident number	**e.g. Hutton/DB/year/001**
Report received by:	
On (date):	
Action taken by responsible officer/s:	

Appendix 2 – Data Security Breach Response Flowchart



Title	General Data Protection Regulation (GDPR) Policy
Author/Creator	Information Governance Officer, Data Protection Officer
Owner	Information Governance Officer
Date Published/Approved	24 May 2018
Version	Final Draft
Date of Next Review	12 Months from published/approval date
Audience	All
Related Documents	GDPR Personal Data Policy
Subject/Description	Following the implementation of the GDPR on 25 May 2018 this policy outlines obligations placed upon the Hutton Group as data controllers in relation to personal data breaches.
Group	Finance and Corporate Services
Department	Research Support