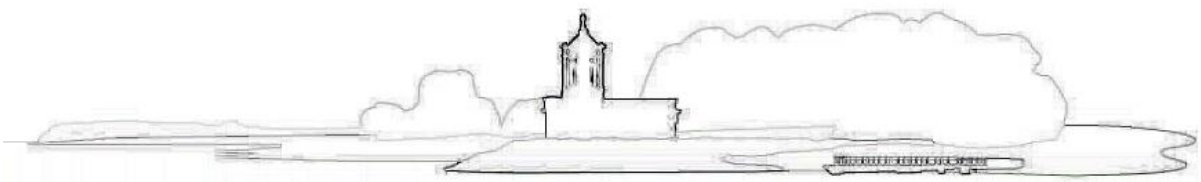
Rutland County Council

DATA INCIDENT RESPONSE POLICY

Version & Policy Number	~~Version one~~ Version two
Guardian	Data Protection Officer
Date Produced	May 2018
Next Review Date	~~June 2019~~

Approved by Cabinet	~~June 2018~~ PENDING APPROVAL



Summary of document

This Policy provides a clear framework in which Members and Officers should operate in the event of a data incident. This Policy should be read in conjunction with other policies and procedures that support the Council's commitment to information governance.

Contents

DATA INCIDENT RESPONSE POLICY

1.1. Policy Statement

Rutland County Council holds large amounts of personal and special data. Every care is taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible.

1.2. Purpose

This Policy sets out the procedure to be followed by all Rutland County Council Members and Officers if a data protection breach takes place.

1.3. Scope

This Policy applies to all personal and special data held by Rutland County Council (see below).

1.4. Legal Context

The United Kingdom General Data Protection Regulations (UK GDPR) makes provision for the regulation of the processing (use) of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

Principle 6 of the UK GDPR ~~General Data Protection Regulations~~ states that organisations which process personal data must take "process in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

1.4.1. Data

Data means information which applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised (for example; key-coded)

1.4.2. Personal Data

Personal data means data which relates to a living individual who can be identified directly or indirectly by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

1.4.3. Special/Sensitive Personal Data

Special/Sensitive personal data means personal data consisting of information as to
The UK GDPR ~~General Data Protection Regulation~~ refers to sensitive personal data as "special categories of personal data" (Article 9 of the ~~General Data Protection Regulations~~ UK GDPR).-

(a) the racial or ethnic origin of the data subject,
(b) his/her political opinions,
(c) his/her religious beliefs or other beliefs of a similar nature,
(d) whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
(e) his/her physical or mental health or condition,
(f) his/her sexual life,
(g) genetic data,
(h) biometric data

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (Article 10 of the ~~General Data Protection Regulations~~ UK GDPR).

1.5. Types of Breach

Data protection breaches could be caused by a number of factors. Some examples are (this list is not definitive):

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as fire or flood
- Hacking
- 'Blagging' offences where information is obtained by deception

2. Breach Management

As soon as the data breach occurs or is discovered, it must be reported by whoever has committed or discovered the breach to their manager and the Data Protection Officer (DPO). The DPO will notify the appropriate senior officers, including the Chief Executive (who will notify the relevant Members) and then launch an investigation into the data breach including appointing a designated Investigation Lead Officer (ILO) who will be responsible for all aspects of the breach investigation process.

2.1. Containment and Recovery

The DPO will coordinate with departmental managers to:

- Establish if the breach is ongoing and take immediate action to stop the breach and to minimise the impact and effect of the breach;

- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise;
- Establish whether there is anything the Council can do to recover any losses and limit the damage the breach can cause;
- Instigate the recovery of physical equipment, where appropriate;
- As far as is practically possible, ensure that Council staff recognise and take action to avoid anyone trying to use the lost or stolen data to access accounts;
- Inform the police, where appropriate;
- Inform the banks/building societies and card providers if appropriate: and
- Inform the Strategic Communications Advisor so that a press statement can be prepared in the event of a media enquiry; depending on the extent and nature of the breach.

If the breach occurs or is discovered outside normal working hours, the investigation and notification of relevant officers should begin as soon as is practicable.

Records must be kept of all actions taken in line with Rutland County Councils ~~Draft~~ Retention and Records Management Policy. The DPO is responsible for collating all records.

2.2. Assessment of an Ongoing Breach

The nature of the breach will determine what steps are necessary in addition to immediate containment. This will be done by an assessment of the risks associated with the breach. This risk assessment will be undertaken by the DPO.

The most important aspect is an assessment of potential adverse consequences for the subject(s) of the data breach, how serious or substantial these are and how likely they are to happen. This will be based on:

- What type of data is involved?
- How sensitive is the data?
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data?
- Regardless of what has happened to the data, what could the data tell a third party about the individual?
- How many individuals' personal data are affected by the breach?
- Who are the individuals whose data has been breached?
- What harm can come to those individuals and/or to the Council?

2.3. Notification of the Breach

The DPO, in conjunction with the relevant Director or Assistant Director ~~Head of Legal and Corporate Governance and the relevant Director or Assistant Director~~ shall determine who will be notified, the information the notification will contain and how they will be notified. In determining the extent of the notification, the following should be considered (this is not an exhaustive list and each breach must be assessed on its own circumstances):

- Which individuals and/or groups, including Council staff, need to be notified?
- What are the dangers of 'over notifying'?

- Any contractual or operational requirements?
- Which regulatory bodies require notification?
- Can notification help the Council to meet its security obligations with regard to the 6 data protection principle?
- Can notification help the subject(s) of the data breach? Bearing in mind the potential effects of the breach, could the subject(s) act on the notification to mitigate personal risks?
- How many people are affected?
- How serious are the consequences?
- How the notification can be made appropriate for particular groups of individuals.

2.3.1 Determining Serious Breaches

The presumption is that all breaches are 'serious' breaches unless the facts of the breach indicate otherwise.

The DPO must determine if the breach is a serious breach that needs to be notified to the Information Commissioner's Office (ICO). This must be done without undue delay and where feasible no later than 72 hours after the breach occurring.

In order to establish the seriousness of a breach the following must be considered:

- The potential harm to the data subject as a result of the breach, including any distress the data subject may suffer as a result of the breach, which is dependent on the volume and the sensitivity of the data involved.
- The volume of the data involved - this must be determined by the facts and extent of the breach.
- The sensitivity of the data involved - where the data is classed as special personal data and the release of that data can lead to the data subject suffering substantial harm.

Serious breaches should be notified to the ICO and the notification should include details of:

- The type of information and number of records
- The circumstances of the loss / release / corruption
- Actions taken to minimise / mitigate effect on individuals involved including whether they have been informed
- Details of how the breach is being investigated
- Whether any other regulatory body has been informed and their response
- Remedial action taken to prevent future occurrence
- Any other information that may assist the ICO in making an assessment

2.4. Evaluation and Response

Once the breach has been dealt with the ILO should evaluate and report to the DPO the effectiveness of the Council's response to the breach.

Where the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing 'business as usual' is not acceptable; similarly, if the Council's response to the breach was hampered by inadequate policies or

a lack of a clear allocation of responsibility then any response must review and update these policies and lines responsibility accordingly.

The evaluation must consider, although not limited to:

- Ensuring those who need to be aware know what personal data is held and where and how it is stored.
- Establishing where the biggest risks lie.
- Ensuring that where data is shared, either internally to the Council or externally, the method of transmission is secure and that only relevant data is shared or disclosed.
- Identifying weak points in existing security measures.
- Monitoring staff awareness of security issues and looking to fill any gaps through training or tailored advice

2.5 Employment Considerations

This Policy should be read in conjunction with the Data Protection Policy and ICT Security Policy and the Code of Conduct.

Where a breach of this Policy has occurred, it may result in action being taken in accordance with the Council's Disciplinary Policy.

3.0 Monitoring and Review

This Policy shall be reviewed every 12 months after implementation.

3.1. Implementation

This protocol was implemented on August 2014

4.0. Contacts

Data Protection Officer 01572 ~~758165~~ 827347

Appendix 1

Rutland County Council

UK GDPR Data Breach Reporting Form
TO BE COMPLETED BY OFFICER REPORTING BREACH

Section A **Minimum information needed about the incident**	
Your contact details	*Name / Job title / Contact phone & email / Team / Department*
Date form completed	
What has happened?	*Provide as much information as possible; The nature of the personal data breach (e.g. transfer to third party not entitled to it, Memory stick lost, etc.)*
How was the incident identified?	*(E.g Notification from member of public, Department, Other organisation, etc)*
What information was put at risk in this incident?	*(E.g. Case file notes of a vulnerable Adult Social Care User)*
Which (if any) of the following does it include? • *Basic personal identifiers (Eg name, contact details)* • *Racial or ethnic origin* • *Political opinions* • *Religious/philosophical beliefs* • *Trade union membership*	

• *Sex life data* • *Sexual orientation data* • *Gender reassignment data* • *Health data* • *Identification data (Eg usernames/passwords)* • *Economic and financial data (Eg credit card/ bank details)* • *Official documents (Eg driving licence)* • *Location data* • *Criminal convictions/offences* • *Genetic or biometric data*	
When was this incident first known by RCC?	*Date and time*
What department and team did the incident occur in?	*Team / Department*
Section B - Continue to complete this section if the incident occurred in your area. If not, then please forward to Information Governance.	
How did it happen?	*Events that led to the incident occurring (E.g. user error, malicious, process not followed, technical issue)*
Where did the incident happen?	*(E.g. At an RCC Office, at staff members' home, travelling etc.)*
When did the incident actually occur?	*Date and time*
Who does the information relate to?	*Brief details about the subject (E.g. frail elderly, looked after child, etc.)*
Does the information contain details relating to any other individuals?	*Yes / No*
If so, how many and in what capacity?	*(E.g. 2 x Family member, 1 x staff, public, agency etc.)*

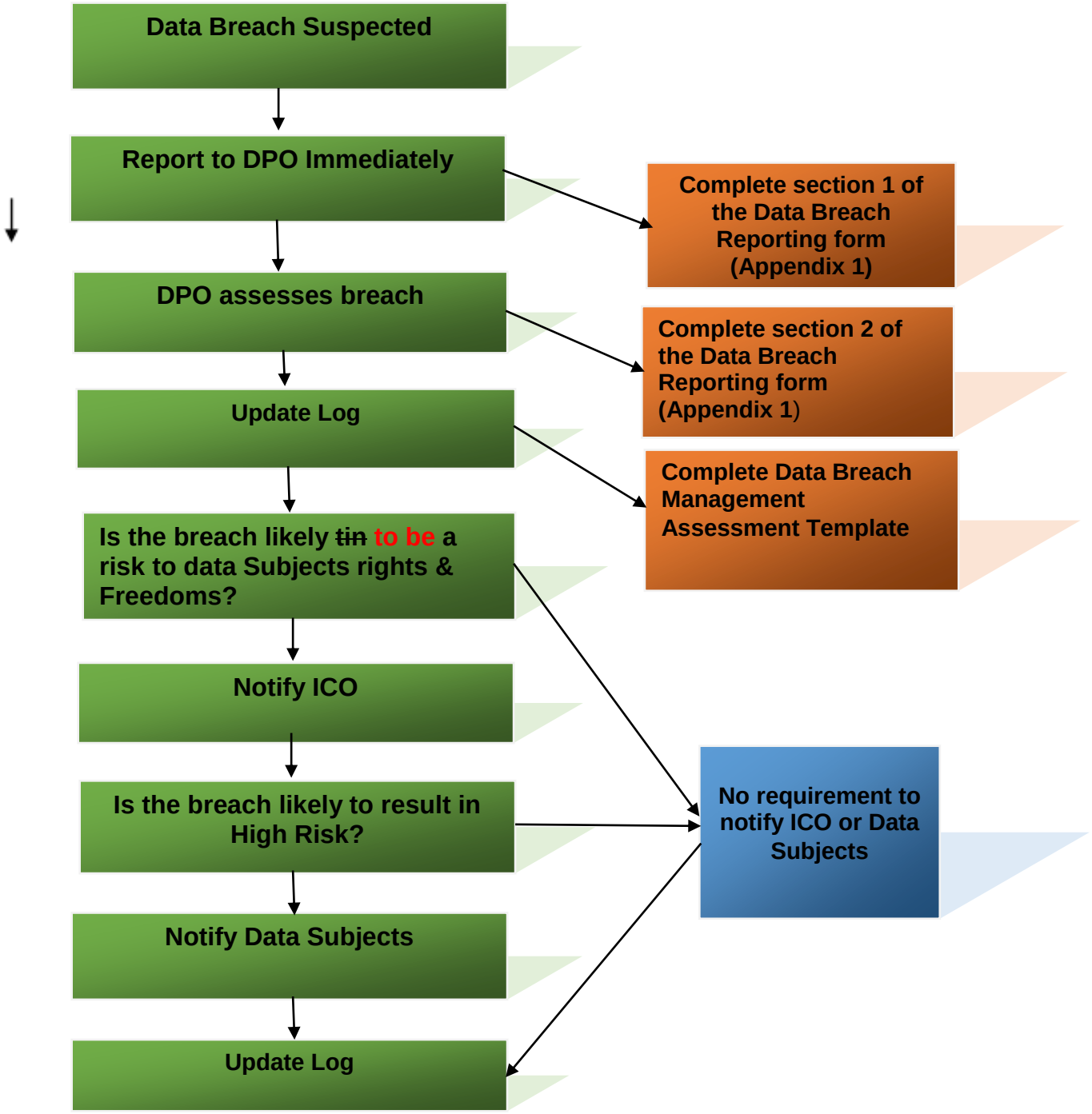
Does it contain confidential information?	*Yes / No*
How many individuals have accessed / received data they were not entitled to see / receive?	*Please also state their status, i.e. staff, public, professional*
Of those individuals mentioned above, what is the relationship to the subject?	*(E.g. Unknown to subject, relative of the subject, carer etc.)*
What format was the information in?	*(E.g. Paper / electronic - If electronic was it encrypted?)*
What is the impact / risk / consequence of the incident? [Potential consequences and adverse effects]	***Potential risks for the subject (s)*** *(E.g. risk of physical/mental harm, embarrassment, fraud/identity theft/financial loss, reputational damage, discrimination, other social/economic disadvantage, loss of confidentiality)*
	Potential risks for Council *(E.g. Loss of reputation, legal action, adverse publicity, etc)*
	Potential risks for public / other *(E.g. Risk of harm, loss of confidence, etc)*
What immediate actions have taken place to deal with the personal data breach?	*List initial actions - Who has been informed? What has been done? Head of Service aware? Information Governance contacted?* *(E.g. retrieved information, asked people to delete – Telephone not by email; Email deleted (deleted Items folder as well; letter collected? etc)*
What measures did the organisation have in place to prevent an incident of this	*(E.g. Policies / procedures / guidance / training)*

nature occurring?	
Do you feel it is necessary / appropriate to inform the data subject/s about the incident? [Team manager in service area to help with decision]	*Yes / No / Already Aware - Please provide reasons for your answer*
Have there been any other organisations involved? If so, have you told, or are you planning to tell them?	*Yes / No / Already Aware - Please provide reasons for your answer*
Are there any further actions to take to prevent the incident happening again?	*Actions for the future – Please give specific, measurable, actions with owners and deadlines*
Have the staff involved in the incident completed the mandatory General Data Protection Regulation training?	*Yes / No* *When?*
Section C - The following section is to be completed by the Information Governance Team	
Incident number	
Completed by	*Member of IG team*
What level of classification does the information fall within?	*See Guide to Information Classification document*
What is the level of risk to an individual's rights and freedoms? • *Negligible Risk* • *Low Risk* • *High Risk* •	
How likely is this risk? • *Improbable* • *Remote* • *Occasional* • *Probable* • *Frequent*	
Does the incident need reporting to the ICO?	*Yes / No (+ any comments re reasoning)*
Severity of incident	*Near Miss Incident / Minor / Major*

Type of breach	*Unauthorised access or disclosure / Corruption or inability to recover data / Disclosed in error / Lost or stolen hardware / Lost or stolen paperwork / Non-secure disposal of hardware / Non-secure disposal of paperwork / Technical Security Failure / Uploaded to website in error / Hacking / Lost in transit / Denial of Service / Phishing email / Social Media Platform / Website defacement / Malicious internal damage / Spoof website / Cyber bullying*
Principle breached	*Lawfulness / Fairness and transparency / Integrity and confidentiality / Accuracy / Purpose limitation / Data Minimisation / Storage Limitation / Accountability*
Are all appropriate technical and organisational measures in place?	*Yes / No*
Date incident closed	

Appendix 2

FLOW CHART



A large print version of this document is available on request.

Rutland
County Council

Rutland County Council
Catmose, Oakham, Rutland LE15 6HP

01572 722 577
enquiries@rutland.gov.uk
www.rutland.gov.uk