West Lindsey
DISTRICT COUNCIL
The Entrepreneurial Council

Information Governance Policy

Data Breach Reporting Policy and Procedure

Document Control

Version Number	Version 2.1
Approved by	Corporate Policy and Resources Committee
Date approved	13/4/2017
Review Date	13/4/2019
Authorised by	Director of Resources
Contact Officer	Strategic Lead - Democratic & Business Support, Central Services

Contents

1. Policy Statement

1.1. West Lindsey District Council ("the Council") processes large amounts of personal and sensitive data. While we take every care to protect personal data we recognise that data breaches occur.

1.2. A breach is defined in Article 4(12) of the General Data Protection Regulation (GDPR) as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

1.3. In the event of a data breach, it is vital we take appropriate action to assess and minimise any associated risk to data subjects as soon as possible. We must report breaches that are likely to result in a risk to individuals' rights and freedoms to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of them. If the breach is likely to result in a **high** risk of adversely affecting individuals' rights and freedoms, then we must inform those individuals without undue delay.

2. Purpose

2.1. This Policy sets out the procedure to be followed by West Lindsey District Council staff, contactors or temporary staff and third party users immediately a data breach is identified.

3. Scope

3.1. This Policy applies to Council staff, contactors or temporary staff and third party users who process personal and sensitive (special category) data held by the Council.

3.2. Personal and special category data are defined in GDPR as follows:

- **Personal Data** – Article 4(1) defines personal data as "any information relating to an identified or identifiable natural person ('data subject') who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.".

- **Sensitive Personal Data** – the GDPR (Article 9) refers to sensitive personal data as "special categories of personal data" e.g. information specifically relating to race or ethnicity; political opinions; religious or philosophical beliefs; trade union membership; physical or mental health or condition; sex life or sexual orientation; genetic data; and biometric data. Personal data relating to criminal convictions and offences are not included but similar extra safeguards apply to its processing (see GDPR Article 10).

3.3. The principles of securing information (in accordance with Principle 6 of the GDPR), can be found in the Council's Information Security Policy.

4. Legal Context

4.1. The GDPR, the Applied GDPR and the Data Protection Act 2018 makes provision for the regulation of the processing (use) of information relating to individuals, including the obtaining, holding, use or disclosure of such information. These instruments come fully into force on 25 May 2018.

4.2. Article 5(1)(e), (Principle 6) of the GDPR states that personal data shall be "processed 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 ('integrity and confidentiality'). ".

4.3. Article 5(2) further states that "The controller [the Council] shall be responsible for, and be able to demonstrate compliance with, [the Principles].". This is the Article 5 principle of "accountability".

5. What is a Personal Data Breach

5.1. Personal breaches are a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Some examples are:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

5.2. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever:

- any personal data is lost, destroyed, corrupted or disclosed;
- if someone accesses the data or passes it on without proper authorisation; or
- if the data is made unavailable and this unavailability has a significant negative effect on individuals.

5.3. Examples of Data Breaches and who to notify when they occur is given at Appendix i.

6. Immediate Containment/Recovery

6.1. The GDPR makes clear that when a security incident takes place, the Council should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

6.2. The following process is shown diagrammatically at Appendix ii.

6.3. A person who discovers/receives a report of an incident involving the confidentiality, integrity, or availability of Council data but which **does not** involve personal information must log an Information Governance Incident on Minerva. This will be investigated in line with the Information Security Incident Management Policy.

6.4. A person who discovers/receives a report of an incident involving the confidentiality, integrity, or availability of Council data **which involves personal information** must inform the ICT Helpdesk immediately. If the incident (breach) occurs or is discovered outside normal working hours, then the ICT Duty Officer (ICT Manager) must be contacted.

6.5. ICT Service Desk staff (or ICT Duty Officer) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, and to alert the relevant team manager or the Out of Hours Duty Officer.

6.6. The ICT Service Desk staff should contact the Data Protection Officer as soon as possible. The Data Protection Officer will provide advice and ensure that an Information Governance Incident is logged and maintained in accordance with the Information Security Incident Management Policy. In order to comply with the GDPR Accountability principle, the Council **must** retain a record of **every** incident involving personal data, regardless of severity.

6.7. The ICT Service Desk staff in consultation with the Data Protection Officer must also consider whether the police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

6.8. The ICT Service Desk staff must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

a. Attempting to recover lost equipment.

b. Contacting the Council's Customer Services Centre, Benefits or other relevant Council Departments, so that they are prepared for any potentially inappropriate enquiries 'phishing' for further information on the individual concerned. Consideration should be given to a global email. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual making the enquiry back.

Whatever the outcome of the call, it should be reported immediately to the ICT Service Desk.

c. Contact the Communications Team so that they can be prepared to handle any press enquiries.

d. The use of back-ups to restore lost/damaged/stolen data.

e. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

f. If the data breach includes any entry codes or passwords, then these codes must be changed immediately, and the relevant agencies and members of staff informed.

g. Following an assessment of the level of risk associated with the incident a decision will be taken as to who will undertake an investigation into the incident.

7. Investigation

7.1. In most cases, the next stage would be for an investigation team comprising the Data Protection Officer, the relevant team manager, and other relevant parties such as the Senior Information Risk Owner (SIRO) and ICT Manager, to be formed to fully investigate the breach.

7.2. The investigation **must** include a risk assessment to establish the likelihood and severity of the resulting risk to people's rights and freedoms. The investigation team must ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation.

7.3. The investigation should consider the type of data, its sensitivity, what protections are in place (eg encryption), what has happened to the data, whether the data could be put to any illegal or inappropriate use, how many people are affected, what type of people have been affected (the public, suppliers etc) and whether there are wider consequences to the breach.

7.4. A clear record must be made of the nature of the breach and the actions taken to mitigate it.

7.5. The investigation must be completed urgently and wherever possible within 24 hours of the breach being discovered/reported. The risk assessment must indicate whether or not the incident needs to be reported to the ICO and, if necessary, the affected data subject(s). A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

8. Notification

8.1. Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once the investigation has taken place.

8.2. If the investigation team's risk assessment indicates that there is a likely risk to the rights and freedoms of individuals, the ICO **must** be notified. The Data Protection Officer is to complete the ICO's Notification Form at Appendix iii as soon as possible.

8.3. If the risk assessment indicates that there is a **high** risk to the rights and freedoms of individuals, then the Data Protection Officer/relevant team manager must inform affected individuals "directly and without undue delay".

9. Review and Evaluation

9.1. Once the initial actions required to contain and report the breach are complete, the Data Protection Officer and the relevant team manager should review both the causes of the breach and the effectiveness of the response to it. A report should be written and sent to the next available Management Team meeting for discussion.

9.2. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources for advice and guidance.

9.3. This Policy may need to be reviewed after a breach or after legislative changes, new case law or new guidance. Consideration should be given to reviewing this policy on an annual basis.

10. Related Documents

- Data Protection Policy
- Information Security Policy
- Information Security Incident Management Policy

11. Implementation

11.1. This Policy takes effect immediately. All managers should ensure that all Council staff, contactors, temporary staff and third party users are aware of this Policy and its requirements. If staff have any queries in relation to the Policy, they should discuss them with their line manager, the Data Protection Officer or the People and Organisational Development Team Manager.

12. Useful Contacts

ICT Service Desk	01427 675165

ICT Manager – ICT Duty Officer (Cliff Dean)	07583033062
Ian Knowles (Senior Information Risk Owner)	01427 675183
Emma Redwood (TM – People and Organisational Development)	01427 676591
Steve Anderson (Data Protection Officer)	01427 676652

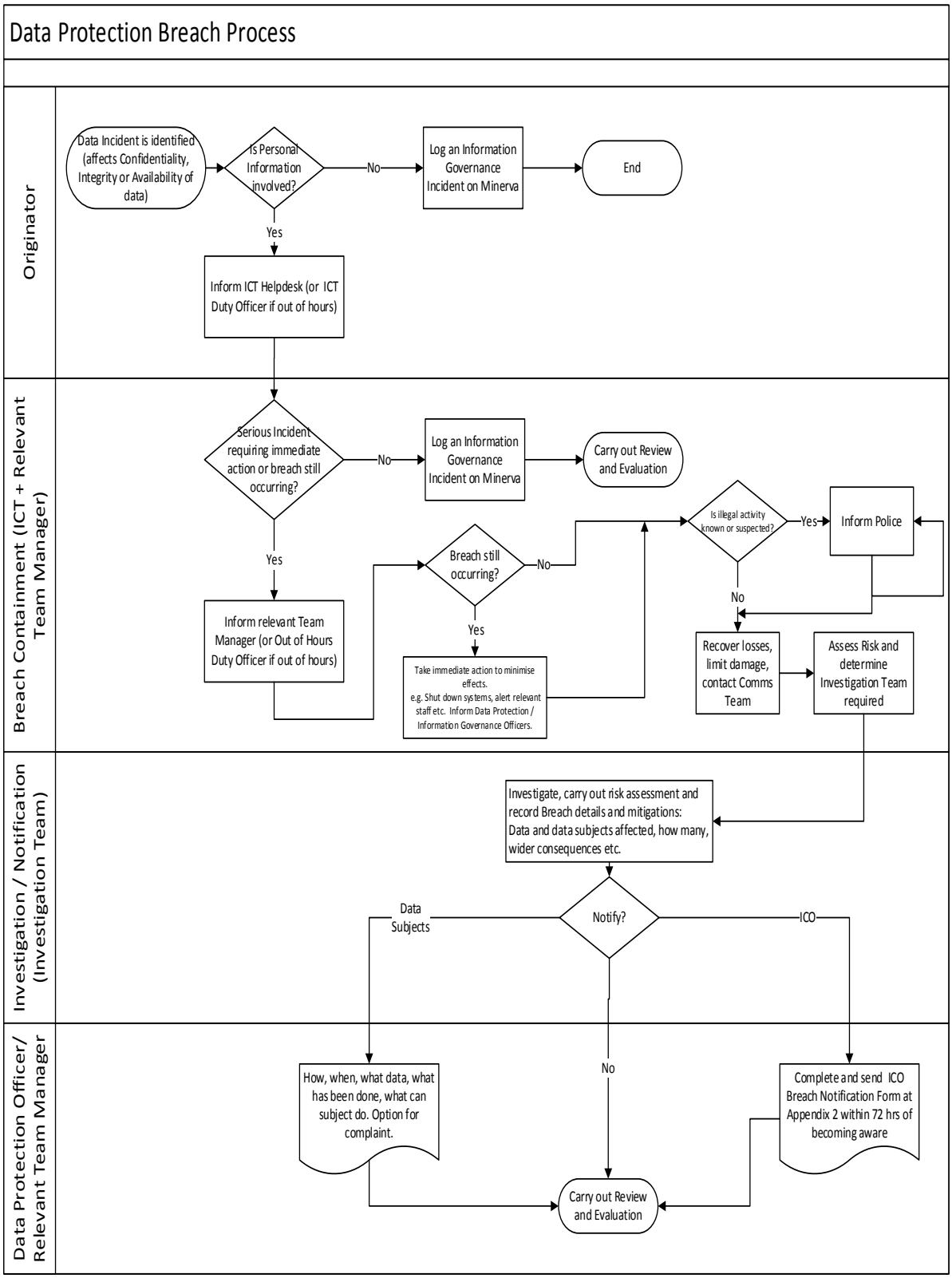
Alternative formats (ie hard copy, large print or Braille) of this procedure are available upon request.

Appendix i – Examples of data breaches and who to notify

Example	Notify the ICO	Notify the data subject	Notes
We stored a backup of an archive of personal data encrypted on a CD. The CD is stolen during a break-in.	No	No	As long as the data are encrypted, backups of the data exist, and the unique key is not compromised, this may not be a reportable breach. However, if it is later compromised, notification is required.
A power outage lasting several minutes at the Guildhall meaning customers are unable to call us and access their records	No	No	This is not a notifiable personal data breach, but still a recordable incident under Article 33(5) of the GDPR. This should be included in the Personal Data Breach Log.
We suffer a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data and that there was no other malware present in the system.	Yes	Only the individuals affected are notified if there is a high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the ICO must be made and the additional step of notifying other individuals if there is a high risk to them.
Personal data of 5000 customers are mistakenly sent to the	Yes	Yes, report to individuals depending on the scope and type	

wrong mailing list with 1000+ recipients		of personal data involved and the severity of possible consequences.	
A direct marketing email is sent to recipients in 'to' or 'cc' field, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the ICO may be obligatory if a large number of individuals are affected, if sensitive data are revealed (e.g. mailing list of a psychotherapist) or if other factors present high risks (e.g. the email contains the initial passwords).	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.
An individual telephones to report having received a benefit letter intended for someone else. We undertake a short investigation (i.e. completed within 24 hours) and establish with reasonable confidence that a personal data breach has occurred and it is a systemic flaw so that other individuals are or might be affected.	Yes	Only the individuals affected are notified if there is a high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the ICO must be made and we take the additional step of notifying other individuals if there is a high risk to them.

Appendix ii – Data Protection Breach Process Diagram



Appendix iii - Data Protection Breach Notification Form

This form is to be used when data controllers wish to report a breach of the Data Protection Act to the ICO. It should not take more than 15 minutes to complete.

If you are unsure whether it is appropriate to report an incident, you should read the following guidance before completing the form: Notification of Data Security Breaches to the Information Commissioner's Office.

Please provide as much information as possible and ensure that all mandatory (*) fields are completed. If you don't know the answer, or you are waiting on completion of an internal investigation, please tell us. In addition to completing the form below, we welcome other relevant supporting information, eg incident reports.

In the wake of a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.

1. **Organisation details**

   (a) * What is the name of your organisation – is it the data controller in respect of this breach?

   (b) Please provide the data controller's registration number. Search the online Data Protection Public Register.

   (c) * Who should we contact if we require further details concerning the incident? (Name and job title, email address, contact telephone number and postal address)

2. **Details of the data protection breach**

   (a) * Please describe the incident in as much detail as possible.

   (b) * When did the incident happen?

   (c) * How did the incident happen?

   (d) If there has been a delay in reporting the incident to the ICO please explain your reasons for this.

(e) What measures did the organisation have in place to prevent an incident of this nature occurring?

(f) Please provide extracts of any policies and procedures considered relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.

3. Personal data placed at risk

(a) * What personal data has been placed at risk? Please specify if any financial or sensitive personal data has been affected and provide details of the extent.

(b) * How many individuals have been affected?

(c) * Are the affected individuals aware that the incident has occurred?

(d) * What are the potential consequences and adverse effects on those individuals?

(e) Have any affected individuals complained to the organisation about the incident?

4. Containment and recovery

(a) * Has the organisation taken any action to minimise/mitigate the effect on the affected individuals? If so, please provide details.

(b) * Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.

(c) What steps has your organisation taken to prevent a recurrence of this incident?

5. Training and guidance

(a) As the data controller, does the organisation provide its staff with training on the requirements of the Data Protection Act? If so, please provide any extracts relevant to this incident here.

(b) Please confirm if training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?

(c) As the data controller, does the organisation provide any detailed guidance to staff on the handling of personal data in relation to the incident you are reporting? If so, please provide any extracts relevant to this incident here.

6. Previous contact with the ICO

(a) * Have you reported any previous incidents to the ICO in the last two years?

(b) If the answer to the above question is yes, please provide: brief details, the date on which the matter was reported and, where known, the ICO reference number.

7. Miscellaneous

(a) Have you notified any other (overseas) data protection authorities about this incident? If so, please provide details.

(b) Have you informed the Police about this incident? If so, please provide further details and specify the Force concerned.

(c) Have you informed any other regulatory bodies about this incident? If so, please provide details.

(d) Has there been any media coverage of the incident? If so, please provide details of this.

Sending this form

Send your completed form to casework@ico.org.uk, with 'DPA breach notification form' in the subject field, or by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Please note that we cannot guarantee security of forms or any attachments sent by email.

What happens next?

When we receive this form, we will contact you within seven calendar days to provide:

- a case reference number; and
- information about our next steps

If you need any help in completing this form, please contact our helpline on **0303 123 1113** or **01625 545745** (operates 9am to 5pm Monday to Friday)