1. Overview

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.
Personal data breaches can include:

- access by an unauthorised third party, as may for example be as a result of an attack on our network.
- deliberate or accidental action (or inaction).
- sending personal data to an incorrect recipient.
- computing devices containing personal data being lost or stolen (Note: in such cases, it will be determined if the loss/theft falls within the scope of this policy)
- alteration of personal data without permission.
- loss of availability of personal data.

Certain types of personal data breach must be reported to the relevant supervisory authority. This must be done **within 72 hours of becoming aware of the breach**, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, those individuals must also be informed without undue delay.

A record must be kept of any personal data breaches, regardless of whether they are required to be notified.

2. Breach Reporting and Management Procedure

1. In any circumstances of personal data breach, suspected breach or alleged breach **DO NOT DO ANYTHING OTHER THAN:**

    1.1. **IMMEDIATELY** notify the Group Human Resources Director (Data Protection Lead), or in their absence, the Group Finance Director (weekend/Bank Holiday contact details below). We will need to know what has happened and determine what to do next, so you are not required to do anything but immediately report it to the Group Human Resources Director (Data Protection Lead), or in their absence, the Group Finance Director. At this stage we will need to be told the following:

    - a description of the nature of the personal data breach including:
        - the categories and approximate number of individuals concerned.
        - the categories and approximate number of personal data records concerned.

- a description of the likely consequences of the personal data breach.
- a description of the measures taken to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

1.2. If personal data has been emailed to an incorrect recipient, **IMMEDIATELY** attempt a recovery, by attempting a recall following the steps in Appendix 1 and sending an email to the unintended recipient in the form set out in Appendix 2. Similar steps can be taken if the personal data breach was not by electronic means.

2. Group Human Resources Director (Data Protection Lead), or in their absence the Group Finance Director to immediately assess and determine:

- whether investigation needs to be conducted.
- likely consequences of the breach – assess risks to individuals.
- what action may be needed.

    - containing the breach
    - obtain ICO advice: 0303 123 1113
    - report to ICO (if likely risk to people's rights and freedoms) https://ico.org.uk/for-organisations/report-a-breach/
    - report to Company insurers
    - report to Police
    - inform individuals (if the personal data breach is likely to result in a high risk of adversely affecting data subjects' rights and freedoms) (Appendix 3)
    - record outcome in data breach record
    - remedial action - better processes, further training or other corrective steps

3. Group Human Resources Director (Data Protection Lead) to record breach outcome. If breach not reported to Group Human Resources Director (Data Protection Lead) all relevant detail must be provided to Group Human Resources Director (Data Protection Lead) by individual to whom the breach is reported.

Weekend/ Bank Holiday contact details:

Text in the following order, until a response is received:

Tracy Pugh, Group Human Resources Director - 07739 325759
John Seaton, Group Finance Director – 07595 279180
Paul Charlesworth, Group IT Manager – 07595 279181

Checklist Procedure to follow in the event of an identified personal data breach, suspected breach or alleged breach

Action required	Responsibility	Done Y/N	Notes
Individual to immediately advise Group Human Resources Director (Data Protection Lead),or in their absence the Group Finance Director, in person, by phone or as a last resort by email.	STAFF		
Individual to provide a written statement summarising the (potential) breach.	STAFF		
Group Human Resources Director (Data Protection Lead), or in their absence, the Group Finance Director, to conduct an investigation into the (potential) 'breach' to ascertain whether personal data and/or sensitive personal data has been compromised and if so how.	Group Human Resources Director (Data Protection Lead), or in their absence the Group Finance Director		
Group Human Resources Director (Data Protection Lead) to provide a written summary on the conclusion of the investigation.	Group Human Resources Director (Data Protection Lead)		
Ascertain what measures (if any) can be put in place to prevent the breach occurring again.	Group Human Resources Director (Data Protection Lead)		
In the event that the conclusion is that client firms should be notified, management team to agree: - how the communication will take place - when the communication will take place	Group Human Resources Director (Data Protection Lead)		
Update the Internal Breach Record	Group Human Resources Director (Data Protection Lead)		
Where appropriate, notify the ICO (72 hours)	Group Human Resources Director (Data Protection Lead)		
Where appropriate, notify the individual	Group Human Resources Director (Data Protection Lead)		

Appendix 1

Email Recall Process in Outlook

1. **Select Sent Items in the left folder pane, then double-click the sent message to open it in a separate window.**
2. **From the ribbon, select. Recall Message, then select OK in the confirmation dialog box.**
3. **Shortly thereafter, you'll receive a Message Recall Report in your inbox.**

Appendix 2

Recall Email

Dear **[DATA SUBJECT NAME]**

I wanted to get in touch about an email that was sent to you in error by me on **[INSERT DATE]**. I apologise, you were sent this email in error, and I should be grateful if you would confirm by replying to this email that you have deleted it **[and its attachment]** from your systems, and that you will not forward, print or use it for any purpose. I apologise for any inconvenience caused and I appreciate your help in this matter.

I want to reassure you that we do take our data protection and confidentiality obligations very seriously and keep our processes under review to ensure that this type of error does not happen again.

Appendix 3

Personal Data Breach Individual Notification Template

(Only if the personal data breach is likely to result in a high risk of adversely affecting data subjects' rights and freedoms)

Dear **[Data Subject]**

Notification of a personal data breach

We are sorry to inform you of a breach of security that has resulted in the **[loss of OR unauthorised disclosure of OR unauthorised access to OR alteration of OR destruction of OR corruption of]** your personal data.

The breach was discovered on **[DATE]** and is likely to have taken place on **[DATE]**.

As a result of our investigation of the breach, we have concluded that:

- The breach affects the following types of information:
    - **[TYPES OF INFORMATION, FOR EXAMPLE, FINANCIAL, SPECIAL CATEGORY DATA, CRIMINAL OFFENCE DATA]**.
- The information has been [**accidentally or unlawfully destroyed OR corrupted OR lost OR altered OR disclosed without authorisation OR accessed by [[NAME OR DESCRIPTION OF ORGANISATION] OR an unauthorised person]]**.
- The breach occurred under the following circumstances and for the following reasons:
    - **[CIRCUMSTANCES].**
    - **[REASONS].**

We have taken the following steps to mitigate any adverse effects of the breach:

- **[MEASURES]**.

We recommend that you take the following measures to mitigate possible adverse effects of the breach:

- **[MEASURES]**.

[We informed the Information Commissioner's Office of the breach on [DATE].]

You can obtain more information about the breach from **[DATA PROTECTION LEAD NAME AND CONTACT DETAILS]**.

We apologise for any inconvenience this breach may cause you. We are extremely sorry that this has happened. Autocraft Solutions Group takes its responsibility to individuals whose personal data we process very seriously, and we are disappointed to have to write to you in these circumstances.

Yours sincerely,

[SIGNATORY]

Autocraft Solutions Group

Document History

Rev	Section	Revision Detail	Author	Approver	Issue Date
1	All	New Policy	T Pugh	J Seaton	28 August 2024