DATA BREACH PROCEDURE

1. INTRODUCTION

(a) This data breach procedure places obligations on London Luton Airport Limited (trading as 'Luton Rising') to take appropriate measures to report potential breaches of personal data and details the course of action to take upon discovery of breach. References in this policy to 'we', 'us' or 'our' means Luton Rising. References to 'you' means any person subject to this policy as identified below.

2. POLICY STATEMENT

(a) Luton Rising maintains personal and special categories of data relating to individuals, employees, stakeholders, consultation participants, campaigners, partners, our organisation and its affairs. We have a responsibility under the UK General Data Protection Regulation ("**UK GDPR**") and the Data Protection Act 2018 ("**DPA**") to protect the security of the personal data we hold.

(b) We are required to put in place appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data as well as protecting the data against accidental loss, destruction or damage.

(c) In the event of a data breach our primary objectives are to:

(i) Prevent the further spread or loss of data;

(ii) Recover the data that has been lost;

(iii) Identify risks arising from the breach;

(iv) Notify appropriate parties of the breach;

(v) Prevent future breaches.

3. SCOPE

This procedure applies to all employees, workers, consultants and contractors working on our behalf. This procedure supplements our policies relating to data protection and information security.

4. RESPONSIBILITY

(a) This procedure is managed by the Data Protection Officer (DPO), who is also responsible for handling personal data breaches under the UK GDPR and ensuring all breaches are recorded and monitored to ensure the appropriate action is taken.

(b) All members of staff are responsible for recognising personal data breaches and reporting any suspected data breaches to the DPO immediately by email to DataProtection@lutonrising.org.uk.

5. DEFINITIONS

Personal Data: any information identifying an individual or information relating to an individual 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 Categories Personal Data. 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: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data.

Processing: means any operation performed on Personal Data, such as collecting, recording, organising, structuring, storing, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Special Category Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

Examples of Personal Data and Special Category Data include:

Personal Data	**Special Category Data**
Full name	Health or disability information
Date of birth	Race or ethnicity
Postal address	Religious beliefs
Email address	Trade union membership
Telephone numbers	Details of criminal offences
Bank details	Details of sex life or sexual orientation
CCTV images	
Financial records	

6. WHAT IS A PERSONAL DATA BREACH?

(a) A Personal Data Breach means any breach of the UK GDPR and/or the DPA leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. Personal Data Breaches could be caused by a number of factors including:

(i) Loss or theft of data or equipment on which data is stored;

(ii) Inappropriate access controls allowing unauthorised access to data;

(iii) Equipment failure;

(iv) Human error; or

(v) Hacking.

(b) Examples of common Personal Data Breaches include:

(i) Sending an email to the wrong recipient

(ii) Losing a USB stick which contains Personal Data

(iii) Having a laptop stolen which contains Personal Data

(iv) Sending a letter or email to the wrong address

(v) Network, phishing, malware or other cyber security incidents

7. ACTIONS UPON DISCOVERY OF A BREACH

(a) On finding or causing a breach, or potential breach, you must report the breach to the Data Protection Officer immediately upon discovery. You must record the details of the breach on the form attached at Appendix 1 and inform the Data Protection Officer of the incident by emailing DataProtection@lutonrising.org.uk.

(b) Upon being informed of the breach, the Data Protection Officer will carry out an assessment of the actions necessary to mitigate any harm that might result from the breach. Each breach will be assessed on an individual basis and any actions taken shall be appropriate to the particular circumstances of the incident in question.

(c) In particular, the Data Protection Officer should take the following actions:

7.1 PREVENT THE FURTHER SPREAD OR LOSS OF DATA

- Identify how the Personal Data Breach occurred and immediately take steps to contain the breach and limit the spread of data. Identifying how the breach occurred will also enable us to take steps to prevent a recurrence of the breach.

7.2 ATTEMPT TO RECOVER THE DATA THAT HAS BEEN LOST

- Identify ways to recover the data. For example, can physical copies of the data be returned, can an email be recalled or can electronic copies be permanently deleted?

7.3 IDENTIFY THE RISKS ARISING FROM THE BREACH

- Consider obtaining specialist legal advice;
- Confirm the amount, sensitivity and type of information in question;
- Identify what security measures were in place when the breach occurred as well as what measures have been put in place following it;
- Confirm who has been put at risk and assess the potential harm resulting from the breach;
- Consider the additional consequences of the breach including loss of reputation, loss of business, liability for fines or contractual breaches.

7.4 NOTIFY APPROPRIATE PARTIES OF THE BREACH

- Consider who to inform about the breach both internally and also externally. (E.g. the police, insurers, and individuals affected.)
- Particular consideration will be given to whether there are any parties that we are legally or contractually obliged to notify (e.g. insurers, regulator).

7.5 NOTIFICATION TO THE ICO

- Assess whether the breach must be reported to the Information Commissioner's Office ("ICO"). This must be judged on a case-by-case basis. To decide, we will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

    - Loss of control over their data;
    - Discrimination;
    - Identify theft or fraud;
    - Financial loss;
    - Damage to reputation;
    - Loss of confidentiality; or
    - Any other significant economic or social disadvantage to the individual(s) concerned.

    If it's likely that there will be a risk to people's rights and freedoms, **we must notify the ICO within 72 hours of the breach occurring**. External legal advice may need to be sought at this stage.

    The decision of whether or not the breach should be reported must be documented, in case it is challenged at a later date by the ICO or an individual affected by the breach.

    Where the ICO must be notified, we will do this via the 'report a breach' page of the ICO website within 72 hours. As required, we will set out a description of the nature of the Personal Data Breach including, where possible:

    - 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; and
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

    If all the above details are not yet known, we will report as much as we can within 72 hours. The report will explain that there is a delay, the reasons why, and when we expect to have further information. We will submit the remaining information as soon as possible.

7.6 NOTIFYING INDIVIDUALS CONCERENED

Consider whether notification to individuals concerned is necessary and beneficial. If a breach is likely to result in a high risk to the rights and freedoms of individuals, then we are required to notify those concerned as soon as possible.

This notification has to be in writing and will set out:

- A description of the likely consequences of the Personal Data Breach;
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual (s) concerned.

When notifying other parties we will consider what information to tell them and how to do so appropriately as to not cause undue harm.

7.7 PREVENTING FURTHER BREACHES

As part of our self-report it is useful to have considered what steps we will take to prevent future breaches. Consideration should be given to the following:

- Assessing data security risks and whether technical or organisational measures could be implemented to minimise these in future;
- Training staff in data security measures; and
- Debriefing any staff involved following the investigation where relevant.

8. IMPLEMENTATION AND REVIEW

This procedure takes effect immediately upon publication and will be subject to a review 2 years after its implementation.

9.CONTACT DETAILS

The Data Protection Officer can be contacted at Data Protection Officer, Hart House Business Centre, Kimpton Road, Luton, LU2 0LA or by email at: DataProtection@lutonrising.org.uk

Name	
Position	
Contact details	
Date	
Time/date of breach	
Time/date of discovery of breach	
Description of data involved	[*provide as much information as possible including the amount, sensitivity and type of information*]
Summary of incident	[*provide a detailed account of what happened*]
Is breach ongoing?	
What steps have been taken to minimise the effects of the breach?	[*confirm any steps taken to rectify the breach*]
Parties affected by the breach	[*include details of those individuals affected by the breach*]
People notified of breach	[*confirm who is aware of the breach, and if relevant how and why they were notified. Do not notify third parties without first discussing the breach with the Data Protection Officer. Confirm whether there has been any media coverage of the breach*]
Details of the investigation	[*confirm the details the investigation into the breach, when is this likely to be completed and what format will it take*]
Signed:	
Name:	
Position:	
Date:	