DATA PROTECTION POLICY

1. INTERPRETATION

1.1 DEFINITIONS:

(a) For the purpose of this Policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, such as an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g., key-coded.

(b) **Sensitive personal data** is referred to in the UK GDPR as **'special categories of personal data'**, which are 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.

(c) For the purposes of this Policy, **processing** refers to any operation performed on personal data such as collecting, recording, organising, structuring, storing, altering, retrieving, using, disseminating, erasing or destroying personal data.

(d) 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	

2. INTRODUCTION

(a) This Policy sets out how London Luton Airport Limited ("we", "our", "us", "Luton Rising") handle the personal data of all individuals we come into contact with in accordance with the UK General Data Protection Regulation (**UK GDPR**) and the Data Protection Act 2018. This includes members of the public, participants in consultations, supporters, suppliers, stakeholders, employees, workers, consultants, volunteers and other third parties and individuals we support.

(b) This Policy applies to all Luton Rising personnel ("you", "your"). You must read, understand and comply with this Policy when processing personal data on our behalf and attend training on its requirements. This Policy sets out what we expect from you for Luton Rising to comply with applicable law. Your compliance with this Policy is mandatory. Any breach of this Policy may result in disciplinary action.

3. SCOPE

(a) We recognise that the correct and lawful treatment of personal data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. Luton Rising is exposed to potential fines of up to £17.5 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the UK GDPR.

(b) All individual business areas are responsible for ensuring all personnel comply with this Policy and need to implement appropriate practices, processes, controls and training to ensure that compliance.

(c) The Data Protection Officer (**DPO**) is responsible for overseeing this Policy and, as applicable, developing any related policies and procedures. The DPO can be contact by emailing DataProtection@lutonrising.org.uk.

(d) Please contact the DPO with any questions about the operation of this Policy or the UK GDPR or if you have any concerns that this Policy is not being or has not been followed.

4. DATA PROTECTION PRINCIPLES

(a) In accordance with the requirements outlined in the UK GDPR, personal data will be:

(i) processed lawfully, fairly and in a transparent manner (**Lawfulness, Fairness and Transparency**);

(ii) collected only for specified, explicit and legitimate purposes (**Purpose Limitation**);

(iii) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (**Data Minimisation**);

(iv) accurate and where necessary kept up to date (**Accuracy**);

(v) not kept in a form which permits identification of individuals for longer than is necessary for the purposes for which the data is processed (**Storage Limitation**); and

(vi) processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (**Security, Integrity and Confidentiality**).

(b) We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (**Accountability**).

5. DATA PROTECTION OFFICER

(a) Luton Rising will appoint a DPO in order to:

(i) Inform and advise Luton Rising and its personnel about their obligations to comply with the UK GDPR and other data protection laws

(ii) Monitor Luton Rising's compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

(b) The DPO will report to the highest level of management at Luton Rising.

(c) The DPO will operate independently and will not be penalised for performing their task.

(d) Sufficient resources will be provided to the DPO to enable them to meet their UK GDPR obligations.

6. LAWFULNESS, FAIRNESS, TRANSPARENCY

6.1 LAWFULNESS AND FAIRNESS

(a) Personal data must be processed lawfully, fairly and in a transparent manner in relation to individuals.

(b) We may only collect, process and share personal data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing but ensure that we process personal data fairly and without adversely affecting the individual.

(c) The UK GDPR allows processing for specific purposes which are set out below:

(i) the individual has given their consent;

(ii) it is necessary for the performance of a contract with the individual;

(iii) to meet our legal compliance obligations;

(iv) to protect the data subject's vital interests;

(v) to carry out a task in the public interest; or

(vi) to pursue our legitimate interests (or those of a third party) for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects. The purposes for which we process personal data for legitimate interests need to be set out in applicable privacy notices.

6.2 SPECIAL CATEGORIES OF PERSONAL DATA

(a) We may only collect, process and share special category data fairly and lawfully and for specified purposes. The UK GDPR allows the processing of special category data for the following specific purposes:

(i) The individual has given their explicit consent;

(ii) The processing relates to personal data manifestly made public by the individual;

(iii) The processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement;

(iv) The processing is necessary for protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent;

(v) The processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity;

(vi) The processing is necessary for reasons of substantial public interest on the basis of UK law which is proportionate to the aim pursued and which contains appropriate safeguards;

(vii) The processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of UK law or a contract with a health professional;

(viii) The processing is reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices; or

(ix) The processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1) UK GDPR.

7. CONSENT

(a) We must only process personal data on the basis of one or more of the lawful bases set out in the UK GDPR, which include consent.

(b) Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

(c) Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

(d) Where consent is given, a record will be kept documenting how and when consent was given so that Luton Rising can demonstrate compliance with consent requirements.

(e) Luton Rising ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

(f) Consent can be withdrawn by the individual at any time.

8. TRANSPARENCY (NOTIFYING DATA SUBJECTS)

(a) The UK GDPR requires organisations to provide detailed, specific information to individuals about the processing of their personal data. The information must be provided through appropriate privacy notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that an individual can easily understand them.

(b) Whenever we collect personal data directly from individuals, we must provide them with all the information required by the UK GDPR including the identity of Luton Rising, how and why we will use, process, disclose, protect and retain that personal data through a Privacy Notice which must be presented when the individual first provides the personal data.

(c) When personal data is collected indirectly (for example, from a third party or publicly available source), we must provide the individual with all the information required by the UK GDPR as soon as possible after collecting or receiving the data.

9. PURPOSE LIMITATION

(a) Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

(b) You cannot use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the individual of the new purposes and they have consented where necessary.

10. DATA MINIMISATION

(a) Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

(b) You may only process personal data when performing your role requires it. You cannot process personal data for any reason unrelated to your role.

(c) You may only collect personal data that you require for your role: do not collect excessive data. Ensure any personal data collected is adequate and relevant for the intended purposes.

(d) You must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with Luton Rising's Data Retention Policy.

11. ACCURACY

(a) Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

(b) You will ensure that the personal data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any personal data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

12. STORAGE LIMITATION

(a) Personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

(b) Luton Rising will maintain retention schedules to ensure personal data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires that data to be kept for a minimum time.

(c) You must not keep personal data in a form which permits the identification of the data subject for longer than needed for the legitimate purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

(d) You will take all reasonable steps to destroy or erase from our systems all personal data that we no longer require in accordance with Luton Rising's Data Retention Policy.

(e) You will ensure individuals are informed of the period for which data is stored and how that period is determined in any applicable privacy notice.

13. SECURITY INTEGRITY AND CONFIDENTIALITY

13.1 PROTECTING PERSONAL DATA

(a) Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

(b) We will develop, implement and maintain safeguards to protect personal data. We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data.

(c) You are responsible for protecting the personal data we hold. You must exercise particular care in protecting special categories of personal data from loss and unauthorised access, use or disclosure.

(d) You must follow all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction. You may only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

(e) You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the UK GDPR to protect personal data.

13.2 DATA SECURITY

The following measures must be taken to protect personal data:

(a) Confidential paper records must be kept in a locked filing cabinet, drawer or safe, with restricted access;

(b) Confidential paper records must not be left unattended or in clear view anywhere with general access;

(c) Digital data must be encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up;

(d) Where personal data is saved on removable storage or a portable device, the device must be kept in a locked filing cabinet, drawer or safe when not in use;

(e) Memory sticks must not be used to hold personal data unless they are password-protected and fully encrypted;

(f) All electronic devices must be password-protected to protect the information on the device in case of theft;

(g) Emails containing special category or confidential personal data must be password-protected if there are unsecure servers between the sender and the recipient; and

(h) Circular emails to stakeholders or individuals must be sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

14. REPORTING A PERSONAL DATA BREACH

(a) The term **'personal data breach'** refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

(b) We have put in place procedures to deal with any suspected personal data breach and will notify individuals or any applicable regulator where we are legally required to do so.

(c) If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Data Protection Officer in accordance with Luton Rising's Data Breach Procedure.

(d) Where a breach is likely to result in a risk to the rights and freedoms of individuals, the Information Commissioner's Office (**ICO**) will be informed. All notifiable breaches will be reported to the ICO within 72 hours of Luton Rising becoming aware of it.

(e) The risk of the breach having a detrimental effect on the individual, and the need to notify the ICO, will be assessed on a case-by-case basis in accordance with our Data Breach Procedure.

(f) In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, Luton Rising will notify those concerned directly in accordance with our Data Breach Procedure.

(g) Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

15. TRANSFER LIMITATION

(a) The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer personal data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

(b) You may only transfer personal data outside the UK if one of the following conditions applies:

(i) the UK has issued regulations confirming that the country to which we transfer the personal data ensures an adequate level of protection for individual's rights and freedoms (e.g. to a country located within the European Economic Area);

(ii) appropriate safeguards are in place such as standard contractual clauses approved for use in the UK or an approved code of conduct or a certification mechanism;

(iii) the data subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or

(iv) the transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between us and the data subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject and, in some limited cases, for our legitimate interest.

16. DATA SUBJECT'S RIGHTS AND REQUESTS

(a) Data subjects have rights when it comes to how we handle their personal data. These include rights to:

(i) withdraw consent to processing at any time;

(ii) receive certain information about our processing activities;

(iii) request access to their personal data that we hold;

(iv) prevent our use of their personal data for direct marketing purposes;

(v) ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

(vi) restrict processing in specific circumstances;

(vii) challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

(viii) request a copy of an agreement under which personal data is transferred outside of the UK;

(ix) object to decisions based solely on automated processing, including profiling;

(x) prevent processing that is likely to cause damage or distress to the individual or anyone else;

(xi) be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

(xii) make a complaint to the Information Commissioner's Office; and

(xiii) in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

(b) You must immediately forward any request from individuals to exercise their data protection rights to the Data Protection Officer in accordance with our Subject Access Request Procedure and our Data Subject Rights Procedure.

17. ACCOUNTABILITY

Luton Rising must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. Luton Rising is responsible for, and must be able to demonstrate, compliance with the data protection principles.

Luton Rising must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

(a) implementing privacy by design when processing personal data and completing data protection impact assessments (**DPIAs**) where processing presents a high risk to rights and freedoms of individuals;

(b) integrating data protection into internal documents including this Policy, related policies and procedures or privacy notices;

(c) regularly training all personnel on the UK GDPR, this Policy, related policies and procedures. Luton Rising must maintain a record of training attendance by Luton Rising personnel; and

(d) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

18. RECORD KEEPING

(a) The UK GDPR requires us to keep full and accurate records of all our data processing activities.

(b) Luton Rising has created, and will maintain, a record of processing activity. This record should include the name and contact details of Luton Rising and the DPO, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place.

19. TRAINING AND AUDIT

(a) We are required to ensure all personnel have undergone adequate training to enable them to comply with data protection laws. We must also regularly test our systems and processes to assess compliance.

(b) You must undergo all mandatory data protection related training.

(c) You must regularly review all the systems and processes under your control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

20. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

(a) We will act in accordance with the UK GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how Luton Rising has considered and integrated data protection into processing activities.

(b) DPIAs will be used to identify the most effective method of complying with our data protection obligations and meeting individuals' expectations of privacy.

(c) A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

(d) A DPIA should be conducted when implementing major system or business changes involving the processing of personal data including:

i. use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

ii. Automated processing including profiling;

iii. large-scale processing of special categories of personal data or criminal convictions data; or

iv. large-scale, systematic monitoring of a publicly accessible area.

(e) Further guidance is set out in Luton Rising's Data Protection Impact Assessment Procedure.

21. AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION-MAKING

(a) Generally, automated decision making is prohibited when a decision has a legal or similar significant effect on an individual unless:

(i) an individual has explicitly consented;

(ii) the processing is authorised by law; or

(iii) the processing is necessary for the performance of or entering into a contract.

(b) If certain types of special category data are being processed, then grounds (ii) or (iii) will not be allowed but the special category data can be processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

(c) If a decision is to be based solely on automated processing (including profiling), then individuals must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the individual's rights and freedoms and legitimate interests.

(d) We must also inform individuals of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the individual the right to request human intervention, express their point of view or challenge the decision.

(e) A DPIA must be carried out before any automated processing (including profiling) is undertaken.

22. DIRECT MARKETING

(a) We are subject to certain rules and privacy laws when marketing to our supporters and members of the public (e.g. individuals who have subscribed to our e-newsletters and updates) and an individual's prior consent is required for electronic direct marketing (for example, by email, text or automated calls).

(b) The right to object to direct marketing must be explicitly provided to individuals in an intelligible manner so that it is clearly distinguishable from other information within a privacy notice.

(c) An individual's objection to direct marketing must be promptly honoured. If an individual opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

23. SHARING PERSONAL DATA

(a) Generally, we are not allowed to share Personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

(b) You may only share personal data we hold with third parties, such as our service providers, if:

(i) they have a need to know the information for the purposes of providing the contracted services;

(ii) sharing the personal data complies with the privacy notice provided to the individual and, if required, the consent has been obtained;

(iii) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(iv) the transfer complies with any applicable cross-border transfer restrictions; and

(v) a fully executed written contract that contains UK GDPR-approved third party clauses has been obtained.

24. CCTV AND PHOTOGRAPHY

(a) Luton Rising understands that recording images of identifiable individuals constitutes as processing personal data, so the use of CCTV is done in line with data protection principles.

(b) Where CCTV is in operation, appropriate signage is put in place to notify individuals that CCTV is in operation in accordance with Luton Rising's CCTV Policy.

(c) All CCTV footage will be kept in line with Luton Rising's CCTV Policy for security purposes for (up to a maximum of 90 days).

(d) If Luton Rising wishes to use images/video footage of individuals in a publication, such as on its website or social media, consent must be obtained from the individual prior to publication.

25. CHANGES TO THIS POLICY

We keep this Policy under regular review and will be reviewed every 2 years, unless there is a change in the law which requires this Policy to be reviewed earlier.

26. RELATED POLICIES AND PROCEDURES

(a) This Policy is implemented in conjunction with the following other policies and procedure:

(i) IT Security Policy

(ii) Data Breach Procedure

(iii) Data Subject Rights Procedure

(iv) Subject Access Request Procedure

(v) CCTV Policy

(vi) Data Protection Impact Assessment Procedure

(vii) Data Retention Policy