# IT SECURITY POLICY

## 1. INTRODUCTION

(a) This Policy sets out the standards London Luton Airport Limited ("we", "our", "us", "Luton Rising") has determined you must observe when using our IT and communications systems, the circumstances in which we will monitor your use, and the action we will take in respect of breaches of these standards

(b) This Policy applies to all Luton Rising personnel ("you", "your") including employees, workers and consultants. You must read, understand and comply with this Policy when using our IT and communications systems. 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.

(c) Luton Rising's IT is provided by Luton Council and this policy is intended to supplement the Council's IT security policies and should be read in conjunction with them. In any instance of conflict the Council's policies shall take precedence.

## 2. RESPONSIBILITY

(a) 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.

(b) The Shared Services Manager is responsible for overseeing this Policy and, as applicable, developing any related policies and procedures.

## 3. EQUIPMENT SECURITY AND PASSWORDS

(a) You are responsible for the security of the equipment allocated to or used by you and must not allow it to be used by anyone other than in accordance with this Policy.

(b) You are responsible for the security of any computer terminal used by you. You should lock your terminal or log off when leaving it unattended or on leaving our premises, to prevent unauthorised users accessing the system in your absence. Anyone who is not authorised to access our network should only be allowed to use terminals under supervision.

(c) You should use passwords on all IT equipment, particularly items that you take out of the office. You must keep your passwords confidential and change them regularly. You must not use another person's username and password or make available or allow anyone else to log on using your username and password. On the termination of employment or other contractual relationship with Luton Rising (for any reason) you must return any equipment, key fobs or cards.

(d) If you have been issued with a laptop, tablet computer, smartphone or other mobile device, you must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. You should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

## 4. SYSTEMS AND DATA SECURITY

(a) You should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).

(b) You must not download or install software from external sources without authorisation from the IT provider. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Incoming files and data should always be virus-checked by

the IT provider before they are downloaded. If in doubt, staff should seek advice from the IT provider.

(c) You must not attach any device or equipment to our systems without authorisation from the IT provider. This includes any USB flash drive, tablet, smartphone or other similar device, whether connected via the USB port, blue tooth connection or in any other way.

(d) We monitor all emails passing through our system for viruses. You should exercise particular caution when opening unsolicited emails from unknown sources or an email which appears suspicious (for example, if it contains a file whose name ends in .exe). Inform the IT provider immediately if you suspect your computer may have a virus. We reserve the right to delete or block access to emails or attachments in the interests of security. We also reserve the right not to transmit any email message.

(e) You should not attempt to gain access to restricted areas of the network, or to any password-protected information, except as authorised in the proper performance of your duties.

(f) You must be particularly vigilant if you use our IT equipment outside the workplace and take such precautions as we may require from time to time against importing viruses or compromising system security. The system contains information which is confidential and subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

**5. USE OF EMAIL**

(a) You should take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Remember that you have no control over where your email may be forwarded by the recipient. Avoid saying anything which would cause offence or embarrassment if it was forwarded to colleagues or third parties or found its way into the public domain.

(b) Email messages are required to be disclosed in legal proceedings or in response to a subject access request in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main server or using specialist software.

(c) In general, you should not:

i) Send, forward or read private emails at work which you would not want a third party to read;

ii) Download or email text, music or any other content on the internet, which is subject to copyright protection, unless it is clear that the owner of such works allows this;

iii) Send messages from another person's email address (unless authorised) or under an assumed name;

iv) Send confidential messages via email or the internet, or by other means of external communication which are known not to be secure;

(d) If you receive an email in error you should inform the sender.

(e) If you send an email to an incorrect recipient in error, you should attempt to recall the message and contact the Data Protection Officer in accordance with Luton Rising's Data Breach Procedure.

(f) Do not use your own personal email account to send or receive email for the purposes of our business. Only use the email account we have provided for you.

## 6. MONITORING

(a) Our systems enable us to monitor telephone, email, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, use of our systems including the telephone and computer systems, and any personal use of them, may be continually monitored by automated software or otherwise. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

(b) We reserve the right to retrieve the contents of email messages or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

(i) To monitor whether use of the email system or the internet is legitimate and in accordance with this Policy;

(ii) To find lost messages or to retrieve messages lost due to computer failure;

(iii) To assist in the investigation of alleged wrongdoing;

(iv) To comply with any legal obligation.

## 7. PROHIBITED USE OF OUR SYSTEMS

(a) Misuse or excessive personal use of our systems or inappropriate internet use will be dealt with under our disciplinary procedures. Misuse of the internet can in some circumstances be a criminal offence. In particular, it will usually amount to gross misconduct to misuse our systems by participating in online gambling, forwarding chain letters, or by creating, viewing, accessing, transmitting or downloading any of the following material (this list is not exhaustive):

(i) Pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

(ii) Offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients or customers;

(iii) A false and defamatory statement about any person or organisation;

(iv) Material, which is discriminatory, offensive, derogatory or may cause embarrassment to others;

(v) Confidential information about us, our business, or any of our staff, clients or customers (except as authorised in the proper performance of your duties);

(vi) Unauthorised software;

(vii) Any other statement which is likely to create any criminal or civil liability (for you or us);

(viii) Music or video files or other material in breach of copyright.

(b) Where evidence of misuse is found, we may undertake a more detailed investigation in accordance with our disciplinary procedure. If necessary, such information may be handed to the police in connection with a criminal investigation.

## 15. 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.