POLICY

Computer Usage & Information Security

Lothian

CONTENTS

1. Scope & Purpose

1.1. Lothian encourages employees to use new technology to enhance business efficiency, performance and customer service, as well as assisting personal development.

1.2. This policy is designed to help you understand our expectations in the use of these business resources and to minimise potential legal or other risks when you use the systems, internet or e-mail at work. In so doing, we trust our employees to behave responsibly and sensibly when using such equipment and software. The purpose of this policy is to assist in the protection of all information assets owned and used by Lothian from the risks posed by inappropriate use. Inappropriate use of information and information systems exposes the organisation to unnecessary risks. Examples include malicious software, virus attacks, the compromise of network systems and services, disclosure of information, regulatory and legal issues.

1.3. All information relating to our customers and business operations is confidential. You must treat paper-based and electronic information with equal care.

1.4. If you have any queries in relation to any of the detail contained within this Policy please discuss them with your Line Manager. Further information on this policy or any other aspects of computer and information security can be provided by the IT Department.

1.5. This policy applies to all employees' of the Lothian Group who use our IT systems with the exception of Training Systems. Agency workers or sub-contractors who are required to use the Company's information systems will also be made aware of and be expected to abide by this Policy.

2. Definitions

2.1. "Communications facilities" includes, but is not exclusive to telephones (mobile and desk), internet, intranet, e-mail, applications, application data, supporting infrastructure and fax. Please note that this list is not exhaustive.

2.2. “Computer” refers to any device that can get direct or indirect access to corporate information such as smart mobiles, PC, laptop or tablet. Please note that this list is not exhaustive.

2.3. “Electronic communications” includes, but is not limited to e-mail, mobile phone calls, text & instant messaging or any other means of communication.

2.4. IT use software to allow “Authorised Users” who have approved authority to perform certain other functions. These users have the authorisation within their specific remits to carry out reasonable tasks to maintain the operation of their IT based systems to ensure the continuous operation of business. These users may be amended as required for legitimate business reasons. “Authorised Users” will be notified by their Line Manager if they are to be allowed these enhanced functions.

3. Principles

3.1. General

3.1.1. Lothian expects its Business Systems to be used in compliance with this Policy; therefore the IT Department uses software and hardware to monitor and record compliance with this Policy.

3.1.2. You may not connect your own laptop, smart device or other computer onto the organisation's network unless authorised by the IT Department and you must inform IT of this action.

3.1.3. Only peripheral devices supplied by the Company (digital cameras, mobile devices etc.) can be installed or configured on any Lothian computer unless authorised by the IT Department.

3.1.4. If you have been given access to the Internet or Email at work, you may use these for limited, private purposes provided no other employee needs to use your computer for work purposes. This use is subject to this

Policy and the rules contained within. The rules about use for work purposes apply equally to personal use.

3.1.5. No system is to be used for your own personal, political or commercial purposes.

3.1.6. When using electronic communications, employees agree not to cause, nor knowingly allow others to cause any nuisance, annoyance or inconvenience to any person by the use of these services or by persistently sending unsolicited communications without reasonable cause. You agree not to use this service for any improper, immoral, fraudulent or unlawful purposes or to send any material which is offensive, abusive, indecent, defamatory, obscene or menacing.

3.1.7. Any attempts by an employee to create and/or distribute malicious programs into the organisation's network (such as viruses, email-bombs, worms, Trojans etc.) are prohibited.

3.1.8. It is policy that only members of the IT Department can carry out the disposal of hardware/software. Any

redundant, faulty or unused hardware or software must be returned to IT.

3.1.9. All confidential items (documents, CD, Data sticks, etc.) must be locked in a secure environment when the area is unattended.

3.1.10. No confidential information must be available for casual viewing or inspection.

3.1.11. All confidential documents must be shredded when ready for disposal or placed in confidential waste bins.

3.1.12. All confidential documents that have been sent to a shared printer must be collected immediately and not left for casual viewing or inspection.

3.1.13. Employees must inform IT of changes to any contract that involves business partners having access to our network or infrastructure so that access can be appropriately managed.

3.2. Internet

3.2.1. Internet access is at management's discretion, the IT Department must receive a formal request. You are not allowed to arrange your own internet access on the PC at your desk. In certain cases (e.g. home study sponsored by Lothian), employees with Lothian issued equipment may be allowed separate internet accounts at home, following approval from IT.

3.2.2. You must not use the Internet to access any inappropriate, sexually explicit or unlawful material. Wherever possible such access will be barred, however, it is impossible to control all access in this way. Anyone deliberately or knowingly accessing such material may face criminal prosecution as well as internal disciplinary action. Examples of unsuitable sites are those related to pornography, illegal drugs, criminal activities, online gambling and some forms of online merchandising, but this list is not exhaustive. Anyone who inadvertently or accidentally accesses such a site should immediately exit it and inform the IT Department as soon as possible. If breached, you may be subject to an investigation and

action may be taken under the Lothian Disciplinary Policy and Procedure.

3.2.3. IT also restricts access to Web log (Blog) sites, however, as above it is impossible to block all sites. Employees should not access non-work related blog sites.

3.2.4. You must not access any site which will incur charges for us, or play games over the Internet.

3.2.5. You must never download any software from the Internet without first referring to and clarifying the software with the IT Department.

3.2.6. If you ever register as a user of a website for work purposes, you must always state that, or click on the option to, confirm that Lothian does not wish to be contacted by any party or in relation to any promotional material.

3.2.7. No user has the authority to enter into a licence or contract terms on behalf of Lothian. Only the IT Department can process any licence or contract application. If in doubt refer to IT.

3.3. Internet Usage for Personal Purposes

3.3.1. Online merchandising is undertaken at your own risk. We do not accept liability for any losses, claims or damages incurred by you as a result of internet access. In addition, we do not accept responsibility for any personal information that you may disclose as a result of Internet access, e.g. credit card details.

3.3.2. If you wish to register as a user of a website for non-work purposes you must not give your own or any colleague's work e-mail address. You must never download any software from the Internet for non-work purposes. The general rules relating to business use access apply equally to use for personal purposes.

3.4. Email

3.4.1. Please check all your messages carefully before sending them, making sure they are accurate and addressed to the correct recipients. It is advisable to prepare longer e-mails off-line before sending them. All outgoing emails bear Lothian's name and if the contents are inappropriate it may affect our reputation or put us at risk of legal or other action.

3.4.2. Staff must not send offensive, demeaning or disruptive messages/ images by email or other messaging platforms. This includes, but is not limited to, messages/images inconsistent with Lothian's Bullying and Harassment Policy and includes without limitation any sexist or racist material or any material which could be offensive on the grounds of a person's disability, age, sexual orientation, religion or belief; to obtain unauthorised or illegal software; to forward electronic chain letters or to post confidential information about Lothian, its staff,
customers or suppliers.

3.4.3. The same rules apply to e-mails as to any other written correspondence so you should take advice if you are unsure in any way about the content of an e-mail. E-mailing of business data to and from a private address is prohibited unless authorised by the IT Department.

3.4.4. If you receive an internal Lothian e-mail which is intended for another person you must notify the sender and/or delete the e-mail immediately. If the e-mail contains confidential information you must not make

use of it or disclose it to anyone else. If there is a breach of confidential information you should refer to the Breach Notification Procedure and notify the Data Protection Officer.

3.4.5. You may not access another user's email without authorisation, as per the Exceptional Circumstances Access Policy. You must not impersonate any other user when using email or amend the content of any message received unless specifically authorised.

3.4.6. You must take particular care with attachments from third parties as these might carry viruses and/or breach copyright rules. If you suspect you have received an email containing a virus you must immediately contact the IT Help desk. Do not forward the suspected email to anyone.

3.5. Telecommunications

3.5.1. Employees should be aware that full details of all calls made (to/from; date; duration and cost) are available on all mobile and fixed line telephones. Excessive usage of telephone systems shall be investigated and appropriate action taken. You may be required to justify any

personal use. So far as is reasonably practicable, the use of mobiles should be minimised with other means of communication, such as desk telephones, being used instead. Call Recording is also present on some phone lines.

3.6. Systems Access and Passwords

3.6.1. Staff must not, without express consent, access a computer or system for which they do not have authority.

3.6.2. All computer users are given a Username and Password; these are unique and must not be shared with any other employee, unless for an express business use. Where people have shared PC's this statement shall not apply.

3.6.3. No user is permitted to log onto any other user's account. In the (unlikely) event that there is a requirement to access another user's account this must be requested via your Line Manager who will request the appropriate approval from IT.

3.6.4. Passwords should be hard to guess and contain at least seven characters. They should include a mixture of

upper and lower case, numbers and special characters (e.g.! # £ $) to strengthen the password.

3.7. Unattended Equipment

3.7.1. Unauthorised access of an unattended workstation can result in harmful or fraudulent use. Equipment should therefore always be safeguarded appropriately – especially when left unattended. IT has implemented controls to help assist the user. If certain devices cannot or do not allow password protected screen-lock they should inform the IT Help desk.

3.7.2. Users are required to screen-lock their computers prior to leaving them unattended. Screen locks/savers must be password protected.

3.8. Software Copyright Compliance

3.8.1. Staff must not copy, attempt to copy or Download Company Licensed Software.

3.8.2. Staff must not give any Company Licensed Software to any third party, including clients and customers without authorisation.

3.8.3. All software must be purchased through the IT Department, who will load the software on the relevant computers or servers. This includes any upgrades to existing applications.

3.8.4. Any employee who suspects that there may be a misuse of software within the organisation should notify the IT Department immediately.

3.8.5. Users are not permitted to bring software from home, or to install or use unauthorised software on Company equipment.

3.8.6. Screen savers can be written as mini programs which can often be scrolling images or graphical images/characters. These are not acceptable as they pose a security risk. The loading of screensavers such as these is prohibited. The loading of any offensive images is not acceptable whether for Wallpapers or any other

reason; examples of acceptable images would be static landscapes/images. If in doubt contact the IT Department.

3.8.7. Company software should not be taken home and loaded onto a user's home computer. If a user has to use software at home for the Company's business, and is not provided with a Lothian computer for this purpose, a separate copy of the software will be bought for the home computer, given that the appropriate authorisation has been obtained. (However, some software companies provide in their licence agreements that home use is permitted under certain circumstances – this will be determined by the IT Department.)

3.8.8. The use of registered Freeware and Shareware may be permitted for appropriate business purposes only, provided it is authorised, sourced and loaded by the IT Department.

3.8.9. All software, information and programmes developed for and/or on behalf of the Company by employees during the course of their employment remain the property of the Company. Duplication or sale of such software without the prior consent of the Company will

be considered an infringement of the Company's copyright.

3.9. Working Remotely

3.9.1. This applies to an employees' use of any Lothian communications facilities whenever you are working on business away from Lothian premises (working remotely).

3.9.2. When you are working remotely, you must:

- Password protect any work which relates to Lothian Buses business so that no other person can access your work; and protect by use of pin number any Smart Device.

- Position yourself so that your work cannot be overlooked by any other person.

- Take reasonable precautions to safeguard the security of your laptop computers, Smart Device's, mobiles and any computer equipment on which you do Lothian Buses' business, and keep your passwords secret.

- Ensure that any work which you do remotely is saved on Lothian Buses' system or is transferred to Lothian Buses' system as soon as is reasonably practicable.

- Ensure that secure ID tags or memory sticks are kept separately from computer equipment when not in use.

3.10. Disclosure of Information Security Information

3.10.1. Employees should not disclose information relating to the organisation's Information Security facilities to anyone outside the business, without Lothian Buses express permission. Any telephone canvassing for information should be passed directly to the IT Department.

3.11. Physical Security Controls

3.11.1. Lothian equipment must not be left unattended. It must not be left in sight in cars, public transport or any public place. Portable equipment must not be kept on desks or in cars overnight; and must be stored in locked cupboard/drawers, if possible or taken home.

3.11.2. Any loss or theft of Company equipment must be reported to your Line Manager, the IT Help desk, and the Police, if appropriate. If the Police are contacted you must ask for and take a note of the incident number.

3.11.3. Only members of the IT Department are permitted to move any non-portable IT equipment, whether within an office or to another site.

3.11.4. The IT Department cannot control anti-virus systems on third party computers. Employees are to ensure that consultants and contractors do not plug their computers onto our network without prior approval. Where possible, non-Lothian employees should make use of a Lothian computer, as opposed to their own equipment. This access will be controlled via the IT Help desk.

3.12. Anti-Virus

3.12.1. All Lothian computers have the organisation's approved anti-virus software installed and scheduled to run at regular intervals.

3.12.2. It is the responsibility of the users to report any viruses found on their computers to the IT Department. If a virus is discovered on a computer, IT will remove the machine from the network until it is verified as virus-free.

3.12.3. Users should never download files from unknown or suspicious sources. All spam emails should be deleted and unknown or suspicious attachments must not be opened.

3.12.4. Users should never attempt to disable their anti-virus software on their computer. If problems arise, the user should contact the IT Help desk for assistance. If breached, the user may be subject to an investigation and action may be taken under the Lothian Disciplinary Policy and Procedure.

4. IT Responsibilities

4.1. A register of authorised software will be maintained by the IT Department. All licences and media will be held centrally.

4.2. The IT Department are responsible for completing the registration of all software with the supplier, installing upgrades and maintaining version control on all software throughout Lothian.

4.3. The IT Department will ensure that all applicable licensing conditions in respect of all software loaded by them are fully met.

4.4. The IT Department use software to grant additional rights to users who have the approved authority to perform certain authorised functions. These authorised users and functions shall be clear and reviewed by line managers periodically.

5. Breach of Policy

5.1. If there is a breach of this Policy, the matter will be investigated and action may be taken under the Lothian Disciplinary procedures. A serious breach of this Policy may constitute gross misconduct and you may be summarily dismissed.

5.2. As part of the investigation you may be called upon to justify the amount of time you have spent on (for example) the Internet or email or the sites you have visited.

6. Version Control

Version No.	Date of Change	Change made by:	Key Amendments
V1.0	18/09/2018	N Connor	Published
V2.0	30/11/2021	N Connor	Reviewed & Published
V3.0	14/11/2023	N Connor	Reviewed & Published