Leasowe Community Centre Trust.

Registered Charity Number 1214971

Public Access Internet Security Policy

1 Introduction

As part of its public service, ***Leasowe Community Centre Trust*** (LCCT) ("the Organisation") provides free public access to the Internet for informational, educational and leisure needs. Sites where such facilities exist are ***Leasowe Community Centre***. When providing the public internet access facility, LCCT recognises its obligation to protect public and organisational information, equipment and systems from threats posed via the internet, malicious conduct and accidental occurrences. This policy details the reasoning for vigilance and the required necessary standards/guidelines with regard to security, when enabling and using public internet access.

2 Purpose

The purpose of this policy is to establish the standards and guidelines by which public internet access will be provided. This will enable systems, data and equipment of both the Organisation and the public to remain as secure as possible. When using publicly available internet access, all employees, contractors, vendors and members of the public should adhere to this policy.

3 Scope

The scope of this policy includes: -

• ICT equipment and systems belonging to, or under the control of the Organisation

• Information in use on the Organisation's ICT equipment, networks and systems.

• ICT equipment and systems belonging to members of the public using the Organisation's public internet facilities.

• The rules, regulations, software and hardware controls incorporated into the provision of public internet access.

• Internet content viewed, copied or circulated by all parties utilising the Organisation's public internet access.

• All parties who use public internet access or parties who enable public internet access, include but not limited to:

o The Organisation's employees

o Third Parties

o Temporary staff

Issue Date January 2026
Review date: January 2027

o Partner organisations

o Members of the public

o Volunteers

4 Responsibilities

Leasowe Community Centre Trust will take all reasonable steps to provide ICT equipment and software with the correct security provisions as a publicly available table top PC at Leasowe Community Centre.

Members of staff are responsible for ensuring that equipment is used by the public in adherence to this policy - therefore enabling internet access whilst minimising security risks.

Members of staff using the Organisation's provided equipment for internet use are required to adhere to this policy.

Members of the public, staff, residents who utilise 'Guest' wireless access points or specially provisioned networked access points whilst using their own ICT equipment should be made aware of this policy – including any damage to privately owned ICT equipment resulting from incorrect usage is their responsibility.

Leasowe Community Centre Trust cannot be held responsible for any financial loss or damage incurred as a result of Internet activity.

Internet content viewed on the Organisation's owned equipment is passed through a filtering mechanism to control access to inappropriate information but ***Leasowe Community Centre Trust*** cannot be held responsible for that content. Users should be aware that the Internet is not a secure medium and that third parties may be able to obtain information regarding user's activities.

5 Policy statement

With the ***Leasowe Community Centre Trust***'s increasing provision of internet access to the public, it is essential that the security and integrity of information and systems is maintained and that the use of internet access facilities in venues is provided on the basis that the creation, accessing, copying, storing, transmitting or publishing of any material that: -

- is sexually explicit or obscene is prohibited.
- is racist, sexist, homophobic, defamatory, harassing or in any other way discriminatory or offensive is prohibited.
- possession of which would constitute a criminal offence is prohibited.
- is either criminal or illegal, or promotes criminal or illegal activities is prohibited.
- contains images, cartoons or jokes that will cause offence is prohibited.

All activity and internet connections managed by ***Leasowe Community Centre Trust*** are monitored and recorded.

Misuse of the facility could result in services being withdrawn or the content of an individual's activity being reported to the Police.

Copies of this policy and advice below should be clearly displayed in areas where public access to the internet is made available.

It is illegal to create, access, copy, store, transmit or publish any materials that fall into the following categories: -

- National Security: instructions on bomb-making, illegal drug production, terrorist activities.
- Protection of Minors: inappropriate forms of marketing, displays of violence or pornography involving minors.
- Protection of Human Dignity: incitement to racial hatred or racial discrimination, harassment.
- Economic Security: fraud: instructions on pirating credit cards.
- Information Security: malicious hacking.
- Protection of Privacy: unauthorised communication of personal data, electronic harassment.
- Protection of Reputation: libel: unlawful comparative advertising.
- Intellectual Property: unauthorised distribution of copyrighted works, e.g. software or music.

In Internet access venues, prior to use of the public internet service, users will be obliged to read and accept the terms of use as above.

Users should be aware that the Organisation has the ability to monitor the use of public internet access facilities and the misuse of the facility could result in services being withdrawn or the content of an individual's activity being reported to the Police.

All ***Leasowe Community Centre Trusts'*** owned equipment designated for use as public internet access systems are secured against theft and damage, installed with malicious code protection software and be recorded on an asset database with an assigned asset tag.

Any member of the public found maliciously interfering with either the Organisation's IT equipment or software used to enable public internet access may be barred from subsequent use of any of the Organisation's Internet Services and ICT facilities. Dependent upon the nature of the incident the matter may also be referred to the Police.

The use of public internet equipment by the Organisation's staff to process the Organisation's information is prohibited, except in exceptional circumstances and with line management approval. Privately owned devices may be used to connect to 'Guest' wireless

access points at designated facilities. No other method of connection is permitted from privately owned devices.

Leasowe Community Centre Trust have implemented appropriate controls to prevent users of the public internet service accessing, installing software or additional hardware on the Organisation's equipment.

The public IT equipment is returned to a default configuration setting on termination of a user session, including the removal of all personal identifiable data.

The equipment available for use by the public has hard drive access removed. Whilst USB ports and read/write CD and DVD drives may be accessible, they will be configured in such a way to stop software being installed onto the Organisation's IT equipment.

6 Breaches of policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to the Organisation's assets.

All employees, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Organisation. In the case of inappropriate use by a member of the public then access rights to the public internet facility may be temporality suspended or permanently removed dependent upon the level of breach that has occurred. In all instances, where potential criminal activity is suspected/reported the matter will be reported to the Police.

In the case of third-party vendors, consultants or contractors, non-compliance could result in the immediate removal of access to the system. If damage or compromise of the Organisation's ICT systems or network results from the non-compliance, the Organisation will consider legal action against the third party. The Organisation will take appropriate measures to remedy any breach of the policy through the relevant systems in place.

In the case of an employee then the matter may be dealt with under the Organisation's disciplinary process.

7 Compliance with legal obligations

The Organisation is bound by the regulations of the Data Protection Act (2018) including the UK General Data Protection Regulations (UKGDPR) and will not release information concerning the use of specific internet resources by any party except as required by law.

The Computer misuse act (1990), The copyright, designs and patents act (1988) the regulation of investigatory powers act (2000) will also apply to equipment used via the Public internet access provision.