CORNWALL EDUCATION
LEARNING TRUST

IT Services Acceptable Usage Policy

Introduction

IT services are provided by Cornwall Education Learning Trust (CELT / the Trust) for academic and business purposes in support of CELT's aims and interests. IT services are made available to a wide range of users on a conditional basis. All users of CELT's services must comply with this Acceptable Use Policy, which additionally incorporates the South West Grid for Learning (SWGfL) Acceptable Use Policy.

Use of CELT's IT is in accordance with this policy. Acceptable use of CELT's IT services is lawful, reasonable and raises no unnecessary risks or security threats for CELT. Unacceptable use is contrary to the Trust's Regulations and will be subject to disciplinary procedures as deemed appropriate.

Increasingly, users of IT, whether they be pupils, teaching staff, affiliates, support staff or partners, access IT services on CELT owned and personally owned devices (sometimes known as BYOD or bring your own device). This policy applies to all forms of CELT's IT services, regardless of who owns the device being used to access IT services.

It is the responsibility of all users of CELT's IT services to read and understand this policy. This policy may be updated from time to time, to comply with legal and policy requirements. This policy does not override national law and all users of CELT's IT services are reminded that they are subject to legal compliance with various statutory requirements including but not limited to the Computer Misuse Act 1990, the Copyright, Design & Patents Act 1988, and the General Data Protection REgulation (GDPR) (Regulation (EU) 2016/679). Users are also reminded that they should read and understand the Acceptable Use policies of non SWGfL or CELT providers for example, Microsoft Office 365, when used in connection with Trust related work, study and research.

1 Applicability & Scope

This policy applies to all use of all IT services administered or supported by CELT, including services provided under contract for CELT. It addresses the use of CELT's hardware and software, network storage, data and resources and connections beyond CELT. It also addresses the use of CELT's assets accessed via resources not fully owned by the Trust, such as partner or research resources and the use of personal BYOD equipment.

2 Policy Statement

Acceptable use of CELT's IT services is lawful, reasonable and raises no unnecessary risks or security threats for the Trust. Particular applications and services may also specify terms of use that should be complied with as a contractual obligation. IT services are provided by the Trust for academic and business purposes. This supports a range of uses that meet CELT's aims and interests and comply with its policies.

Personal use is not offered as a right and must never interfere with the Trust's work. It should be incidental and modest and cause CELT no risk or unnecessary expense.

Acceptable Use

- Registered users are encouraged to use the Trust's IT services to further the goals and objectives of the school related work, study and research.
- 'Personal use' of the Trust's IT services is permitted but only on a conditional basis providing it does not cause unwarranted expense, risk or liability, or reputational damage to the Trust, to be incurred by the Trust or otherwise impact upon the delivery of services to others through its scale or nature.
- Users should be aware that they are subject to any regulations applicable at a remote site when accessing the Trust's IT services, or to any regulations governing the use of a specific application or service.
- Acceptable use must comply with the the SWGfL Acceptable Use Policy: Internet access and related services are provided to the Trust by SWGfL (South West Grid for Learning). Users must comply fully with SWGfL's Acceptable Use Policy when connecting beyond the Trust. Under the SWGfL Acceptable Use policy User Organisations (such as the Trust) and its members can use the SWGfL network for any lawful activity in furtherance of the missions of the User Organisation. All use of SWGfL is subject to the SWGfL Terms. For detailed information on the SWGfL Terms, a link to this policy is included in the Related Policies & Other Documents section below.

Unacceptable Use

- Unacceptable use includes, but is not limited to, the following activities (other than for properly supervised and lawful research purposes) some of which may be unlawful in certain circumstances:
- Creating, transmitting, storing or displaying offensive, indecent or obscene material.
- Creating, transmitting or displaying of material that deliberately and unlawfully discriminates, or encourages deliberate and unlawful discrimination, on the grounds of race, ethnicity, gender, sexual orientation, marital status, age, and disability, political or religious beliefs.
- Creating or transmitting defamatory material.
- Obtaining, transmitting or storing material where this would breach the intellectual property rights of another party. This includes downloading and sharing music, video and image files without proper authority.
- Creation or transmission of material with the intent to defraud.
- Commercial uses unrelated to the interests of the Trust.
- Uses of the the Trust's email system that is likely to cause annoyance or inconvenience, e.g. sending unsolicited email chain letters.
- Inappropriate or careless use of data e.g. sharing information when not authorised to do so (especially personal and sensitive personal data), or emailing information to the wrong recipient.
- Deliberate activities with any of the following characteristics:
    - Wasting staff effort or IT service resources.
    - Corrupting or destroying another user's data or violating their privacy.

- Using the IT services in a way that denies services to other users.
- Deliberately introducing, executing or transmitting malware.
- Deliberately disabling or compromising the Trust's IT security systems.
- Physical or other damage to IT services.

3 Legal and Compliance Duties

The Trust has a statutory duty to comply with all relevant statues, including GDPR and Prevent.

The Prevent Duty
The Trust has a statutory duty, under the Counter Terrorism and Security Act 2015, termed 'PREVENT'. The purpose of this duty is to aid the process of preventing people being drawn into terrorism. You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. The Trust reserves the right to block or monitor access to such material.

4 Ownership & Asset Management of the Trust's IT

- All IT services provided by the Trust, directly or via other funding, shall be considered as an IT asset, whether directly owned or leased.
- All CELT IT assets may be tagged and inspected as required.
- All CELT IT assets shall be returned to IT services upon request, or when a user leaves the Trust.
- All CELT IT assets may be tracked and recorded in the Trust's asset systems irrespective of their geographic location.

5 Exemptions from Unacceptable Use

Where use of IT Services for what would otherwise be an unacceptable use of these services is required for CELT related business (such as lawful research), the user should notify their Head of Department or relevant member of SLT, ELT or the Board as appropriate. Advice on the application of certain legislation as it applies to the use of IT can be sought from the Trust appointed Data Protection Officer: dpo@peninsulatrust.org

6 Enforcement

Any registered user found to have violated this policy will be in breach of the Trust's Regulations. Breaches shall be subject to initial investigation by IT Services and should be reported to the CIO (cio@peninsulatrust.org), as a security incident. Breaches of this policy will also be subject to disciplinary procedures as deemed appropriate.

Many activities described in this policy have the potential also to be regarded as a breach of criminal law. The Trust shall cooperate in any Police enquiry, and shall report any matter which appears to constitute a serious criminal offence, or where otherwise the Trust thinks fit to do so, directly to the Police.

The Trust also has a statutory duty, under the Counter Terrorism and Security Act 2015, termed 'PREVENT'. The purpose of this duty is to aid the process of preventing people being drawn into terrorism.

7 Responsibilities

Role	**Responsibility**
Users of CELT IT Systems, information systems and networks.	Members of the Trust using Trust information systems and networks will act lawfully and responsibly and in full compliance with all relevant policies and procedures when handling and sharing Trust data, in whatever format (i.e. digital or physical). Third parties who manage, process, transmit or store information, or information system on behalf of the Trust will act responsibly and in full compliance with this Policy and all relevant policies and procedures when handling and sharing Trust data.
IT Services Team	Responsible for: • Administering access to Trust's Active Directory environment and many of its systems • Hardening end user systems • Implementing role based access control upon the Trust's shared access file systems • Creating the Trust's Active Directory user accounts, maintaining network infrastructure, firewalls and network zoning
Governance	The Trust's Executive Leadership Team (ELT) supported by the Chief Information Officer (CIO) ensures that security is properly evaluated and managed across the Trust. IT Governance is responsible for: • Writing and maintaining this policy

	• Investigating security incidents and breaches and recommending remedial actions • Assessing information and security risks. • Identifying and implementing controls to risks.

This policy is monitored by the Trust's Audit committee and reported to the Board.

Related Documents

IT InfoSec Policy	<TBC>
IT Network Policy	<TBC>
PCI DSS Standard v3.2	https://www.pcisecuritystandards.org/document_library
The Computer Misuse Act 1990	https://www.legislation.gov.uk/ukpga/1990/18/contents
The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000	http://www.legislation.gov.uk/uksi/2000/2699/contents/made
Data Protection Act 1998	https://www.legislation.gov.uk/ukpga/1998/29/contents
General Data Protection REgulation (GDPR) (Regulation (EU) 2016/679)	http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
The Copyright Designs and Patents Act 1988	https://www.legislation.gov.uk/ukpga/1988/48/contents
SWGfL Schools Internet Service User Agreement	https://swgfl.org.uk/Uploads/28/2810f93f-f881-4ba7-871e-eb2e481415c8.pdf

History of Changes

Version	Date	Page	Change	Origin of Change
1.0	16/04/18		Original Draft	CIO
2.0	01/11/19		Updated PLT to CELT	CELT IT Manager