Acceptable Use (ICT) Policy

Emil Dale ACADEMY

This policy is applicable to all of Emil Dale Academy's (EDA)* staff**and students on any full-time course.

**In this policy, the abbreviation of EDA will be used to cover all business streams.*

*** In this policy the term "staff" covers all individuals undertaking work or services for the company regardless of their employment status.*

1. Introduction and Aims

ICT is an integral part of the way EDA works and is a critical resource for students and staff alike. It supports teaching and learning, pastoral and administrative functions of EDA,

However, the ICT resource and facilities that EDA uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the acceptable use of EDA ICT resources for students and staff;
- Establish clear expectations for the way that all members of the EDA community engage with one another online;
- Support EDA’s policy on data protection, online safety and safeguarding;
- Prevent disruption to EDA through the misuse, or attempted misuse of ICT systems; and
- Support EDA in teaching students safe and effective internet and ICT use.

2. Definitions

"**Purpose for permitted use**" - You may use the EDA network and email systems to:

1. Conduct solely EDA work;
2. Communicate with students and staff;
    a. Any communication between a student and staff member should only take place on either the EDA Microsoft Teams channels or by official EDA emails.
3. Access material solely for the purpose of conducting EDA work; and
4. Download material solely for the purpose of conducting EDA work.

"**ICT facilities**" - Includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service.

"**Users**" - Anyone authorised by EDA to use the ICT facilities.

"**Personal use**" - Any use or activity not directly related to the users' employment, study or purpose.

"**Authorised personnel**" - Employees authorised by EDA to perform systems administration and/or monitoring of the ICT facilities.

"**Materials**" - Files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs.

3. Policy

The use of the EDA IT network (including hardware, email, database, computer and software systems - for the purposes of this document, called "the network") must only be used in accordance with the purpose for the permitted use.

3.1 Unacceptable use

The following is considered unacceptable use of EDA's ICT facilities by any member of the EDA community. Any breach of this policy may result in disciplinary or behavioural proceedings (see Section 3.3 below). You may ***not*** use the network for any of the following purposes:

a. Using EDA's ICT facilities to breach intellectual property rights or copyright;
b. Using EDA's ICT facilities to bully or harass someone else, or to promote any form of discrimination;
c. Breaching any of EDA's policies and/or procedures;
d. Any illegal conduct, or statements which are deemed to be advocating illegal activity;
e. Accessing, creating, storing, linking or sending material that is pornographic, offensive, obscene or otherwise inappropriate;
f. Activity which defames or disparages EDA, or risks bringing EDA into disrepute;
g. Activity which aims to manipulate and/or alter assessments, grades or transcripts;
h. Sharing confidential information about EDA, its pupils, its staff, or any other member of the EDA community;
i. Setting up any software, applications or web services on EDA's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data;
j. Disrupting the work of other users; using the network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
k. Continuing to use an item of networking software or hardware after a request that use cease because it is causing disruption to the correct functioning of the network;
l. Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel;
m. Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to EDA's ICT facilities;
n. Removing, deleting or disposing of ICT equipment, systems, programs, or information without permission by authorised personnel;
o. Causing a data breach by accessing modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation;
p. Using inappropriate or offensive language;
q. Promoting a private business, unless this has been approved by authorised personnel; and
r. Using websites or mechanisms to bypass EDA's filtering mechanisms.

This is not an exhaustive list. EDA reserves the right to amend this list at any given time. EDA's Senior Management team will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of EDA's ICT facilitates.

3.2 Exceptions from unacceptable use

a. Where the use of EDA ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Principal's discretion, e.g. access to materials needed for research that would otherwise be blocked by the filtering system.

3.3 Sanctions

Students and staff who engage in any of the unacceptable activities listed above may face disciplinary action or receive appropriate sanctions in line with EDA's policies.

Where necessary, and at the sole discretion of EDA, access by an individual or organisation may be withdrawn, either temporarily or indefinitely.

In the event of misuse of the network EDA reserves the right to exclude access to any external organisation, or employee, or student and in the case of:

a. Misuse by an employee of EDA, to proceed against that employee under EDA's disciplinary procedures for employees; and
b. Misuse by a student, to proceed against that student in accordance with EDA's Student Disciplinary Procedures.

3.4 Use of phones and email

a. EDA provides each student and resident member of faculty with an official EDA email address and access to an EDA specific Microsoft Teams account. These accounts should be used for official EDA purposes only. All EDA-related business should be conducted using the accounts that EDA has provided.
b. Individuals must take care with the content of all EDA emails and Teams posts/comments, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of student and/or staff contracts and handbooks.
c. Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Ac 2018 in the same way as paper documentation. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should therefore be treated as potentially retrievable.
d. If an individual receives an email in error, the sender should be informed and the email, deleted. If the email and/or Teams post contains sensitive or confidential information, the user must not make use of that information or disclose that information.
e. If an individual sends a communication in error with contains any form of personal information of another person, they must inform EDA's Data Protection Officer (Sarah Moore) immediately and follow EDA's data breach procedures.
f. Students must not give their personal email addresses, phone numbers, or social media handles to staff members. Staff members, in turn, must not give such information to students either.
g. EDA internal phone lines must not be used by staff for personal matters.

3.5 Monitoring of the EDA network and ICT facilities

a. It is beyond the resources and ability of EDA to monitor all activities on the network. However, where there is sound reason to suspect unacceptable use as defined above, EDA reserves the right to inspect a user's material and use history, including email messages, and at its sole discretion block or edit such material as it sees fit.

b. Furthermore, from time to time, EDA may implement technical measures to monitor activity on the network to ensure compliance with the requirements of this Policy and to carry out tests for research purposes.

3.6 Data security

EDA takes steps to protect the security of its computing resources, data and user accounts.

a. EDA cannot guarantee security. Students, staff and any other individual who use EDA’s ICT facilities should use safe computing practices at all times.

3.6.1 Passwords

b. All users of EDA’s ICT facilities should set strong passwords for their accounts and keep these passwords secure.

c. Individuals must not share the passwords for any of their EDA accounts.

d. Account owners are held responsible for all activities and content associated with their accounts.

e. Failure to conform to these requirements may lead to the suspension of account privileges or other actions as provided by the appropriate EDA policy.

f. If an individual believes that someone else is accessing their account, they must report this immediately to their Line Manager or Course Leader.

3.6.2 Access to facilities and materials

a. Users should always log out of systems and lock their equipment when they are in in use to avoid any unauthorised access.

b. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

4. Related policies

This policy should be read alongside EDA's policies and/or procedures on:

- EDA Student Privacy Notice
- EDA Information Security Policy
- EDA Information Handling Policy
- Staff Code of Conduct Handbook
- Student Code of Conduct and Handbook
- Staff Disciplinary and Grievance Procedure

Version Number	**Date of Issue**	**Review Date**	**Author**	**Changes Made/ detail**
01	12th August 2020	June 2021	Sarah Moore	First issue
02	8th August 2022	July 2023	Eden Tinsey	Annual policy review
03	20th June 2023	July 2024	Eden Tinsey	Policy review and re-write