English Path
891 Greenford Rd,
Greenford, London,
United Kingdom
UB6 0HE

+44 (0) 207 539 3548
info@englishpath.com
www.englishpath.com

To create the world's most accessible and innovative language school that changes lives through education.

English Path Global ICT Policy
Code of Practice for the Use of Information Computing Technology Facilities (ICT)

Version History

Version	Author	Reviewed by	Pages	Approved by	Date published
3	Head of ICT	-	11	Mike Summerfield (Managing Director)	12.06.2025
2	Head of ICT	Juliette Synnott – Lee	7	Mike Summerfield (Managing Director)	06.09.2023
1	Head of ICT	Mike Summerfield	7	Mike Summerfield (Managing Director)	28.05.2021

Introduction

This policy outlines the principles, responsibilities, and conditions governing the use of Information and Communications Technology (ICT) at English Path (EP). It ensures the secure, ethical, and effective use of digital resources by staff, students, and partners across all EP campuses. The policy supports compliance with legal and accreditation standards, and contributes to a safe, inclusive, and digitally responsible learning environment. This policy is aligned with applicable accreditation standards including British Council Criteria 2024, QQI ELE Code 2024, and Eaquals Version 7.3.

Contents

1. Purpose

1.1 To provide a policy for the use of information computing technology facilities owned and provided by English Path (EP from now on) for staff, students, and other stakeholders.
1.2 To ensure that EP's ICT facilities are used in a secure, ethical, and effective manner to support learning, teaching, administration, and communication.
1.3 To provide clear expectations around responsible use, including safeguards for the wellbeing of all users, particularly minors, and the protection of EP's digital environment.

2. Scope, Background and Applicability

2.1 Scope

This ICT Policy concerns all computer systems, network and Wi-Fi facilities operated by EP at all its campuses and regardless of location, where responsibility for user management and control resides with members of staff of EP, or where it may be outsourced to third parties.

2.2 Background

This policy document has been developed to help ensure that EP's information computing technology, in its widest sense, is protected against unauthorised use and unauthorised access. In particular, the policy has been developed to help ensure protection against unauthorised access and modification to EP's various data systems and other ICT systems. It is also intended to support compliance with regulatory requirements and internal quality assurance expectations.

2.3 Applicability

This policy concerns:

- The use of EP owned ICT facilities, including information systems
- EP network facilities (wired and wireless) regardless of whether these are used through the connection of EP owned equipment or through the connection of private equipment to EP owned equipment

This policy applies to:

- All full-time, part-time and temporary staff employed by, or working for or on behalf of EP
- All students studying at EP
- Contractors and consultants working for EP
- All other individuals or groups, including visitors, who have been granted access to EP's ICT facilities

It is the responsibility of each person to whom this policy applies to fully adhere to its requirements. Local adaptations to this policy may apply at international campuses in line with relevant national legislation, but the core principles remain applicable across all EP locations.

3. Definitions

For the purpose of this policy, the following terms are defined as:

- **Authorised Use** – Use of EP ICT facilities by individuals who have been granted access in accordance with the conditions set out in this policy.
- **Digital Safeguarding** – Measures to protect users, particularly minors, from online harm, inappropriate communication, or exploitation through digital channels.
- **EP** – Refers to English Path, including all campuses and locations operating under the EP brand, regardless of geographic location.
- **ICT (Information and Communications Technology)** – Refers to all computer systems, software, networks, internet access, email services, and communication tools provided or authorised by EP.
- **ICT Facilities** – Includes all hardware, software, data systems, Wi-Fi networks, learning platforms, email systems, and digital resources managed or owned by EP.
- **Incident/Breach** – Any event that compromises the confidentiality, integrity, or availability of ICT systems, or which involves misuse, data loss, or unauthorised access.
- **Monitoring** – The lawful process by which EP may review user activity on its ICT facilities to ensure compliance with this policy and applicable laws.
- **Personal Device** – Any privately owned electronic device used to access EP's systems or Wi-Fi, such as laptops, smartphones, or tablets.
- **Unauthorised Access** – Any attempt to access, modify, or interfere with ICT systems, data, or resources without explicit permission.
- **User** – Any individual who has been authorised to access EP ICT facilities, including staff, students, contractors, visitors, and external partners.

4 Responsibility

4.1 The Managing Director has overall responsibility for the implementation and maintenance of this policy.
4.2 Day-to-day responsibility for ensuring compliance with this policy across all EP campuses rests with the Head of School at each location, who may delegate specific tasks to appropriate personnel such as ICT Managers, Systems Administrators, or Compliance Officers.
4.3 The Global ICT Lead (or equivalent central role) is responsible for:

- Ensuring the security and integrity of EP's ICT infrastructure
- Overseeing updates to this policy in line with legislative or accreditation changes
- Coordinating ICT-related training and awareness for staff
- Supporting risk management and incident response protocols

4.4 All users of EP's ICT facilities are responsible for:

- Familiarising themselves with and adhering to this policy
- Reporting ICT security incidents or inappropriate usage
- Taking reasonable steps to safeguard their own use of EP ICT systems

4.5 Where minors are involved, all staff must also comply with the EP Safeguarding and Prevent Policy.

4.6 All staff should complete induction training on EP's ICT policy and related digital responsibilities and participate in periodic refresher training as required.

5 Policy and Procedures

A Code of Practice for the Use of EP ICT Facilities

Conditions of use of EP's computer systems

You may use EP's ICT and Wi-Fi facilities if you are:

- An employee of EP
- A student registered for a programme of study at EP
- An individual or a member of a group who has been permitted to use the EP's ICT
- A visitor to EP

Only the Chief Executive Officer or Head of School may authorise individuals or groups to use and access EP's facilities. All users are expected to behave in a responsible, lawful and ethical manner at all times.

Use of private equipment

Privately owned equipment of staff, students and other individuals or groups may only be connected to EP's Wi-Fi upon agreement of either the Chief Executive Officer or Head of School. EP accepts no responsibility for the effects that any such connection may have on the operability of privately owned electronic or other devices, consequently all risks, however small, reside with the owner. Privately owned devices must not be used to bypass security protocols or access systems unless expressly permitted. Any personal device used to connect to EP systems must be password-protected and maintained in line with EP's minimum-security expectations.

Laws and regulations

All use of EP's ICT facilities must be in full compliance with English law, and where appropriate, all other regulations which are applicable. You must not try to gain unauthorised access to any computer system anywhere at EP. This is commonly known as hacking and constitutes a criminal offence under The Computer Misuse Act 1990. In certain cases, such activities can also be contrary to other legislation, for example, The Terrorism Act 2000.

You must not do anything maliciously, negligently or recklessly which might cause any sort of harm or disruption to any computer system anywhere (worldwide), or to any of the programs or data on any system. In this context the word harm is taken to mean any kind of damage, and any kind of unauthorised access, denial of resources or any data alteration.

If you are reasonably requested to do so, you must justify your use of EP's ICT facilities and/or Wi-Fi facilities. You must explain (in confidence, if necessary) what you are doing, and how and why you are doing it. You must make any reasonable changes requested by senior staff and comply with any reasonable restrictions placed upon you.

You must comply with valid regulations covering the use of software and datasets, whether those regulations are made by law, by the producer or supplier of the software or datasets, by EP, or by any other legitimate authority. Where you have any doubts you must contact the Head of School before using EP's ICT facilities.

The Data Protection Act 1998 regulates the use and storage of personal information (i.e. any information which identifies a living individual) on computing systems. It is your responsibility to ensure that your information and computer usage complies with this law. Failure to do so could result in criminal charges being brought against both you and EP. (Note: GDPR and Data Privacy are addressed in related EP policies.)

Whilst every reasonable endeavour is made to ensure that the ICT facilities and Wi-Fi facilities are available as publicised and scheduled and function correctly, no liability whatsoever can be accepted by EP for any direct or consequential losses or delays as a result of any system malfunction.

Conditions applicable to all EP ICT users

EP's ICT facilities must not generally be used for, or in connection with, the activities identified below, some of which could result in legal action or civil proceedings being mounted against either an individual, EP, or both:

(a) Deliberately accessing, creating or transmitting any obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material, except where the sender/recipient would expect to exchange such material in a professional capacity for official EP work or research.

(b) Creating, transmitting or accessing material which is designed or likely to cause offence, annoyance, inconvenience or needless anxiety to another.

(c) Creating, transmitting or accessing material which runs the risk of drawing people into, or towards, terrorism and/or extremism, except where it can be demonstrated that there is a legitimate academic interest.

(d) Deliberately contributing to News Groups or web sites that advocate illegal activity.

(e) Creating or transmitting defamatory material or material that is libellous of any other person's or company's reputation, products or services.

(f) Viewing, transmitting, copying, downloading or producing material, including software, films, television programmes, music, documents and books which infringes the copyright of another person or organisation.

(g) Making offensive or derogatory remarks about staff, students or EP on interactive websites such as Facebook, X, YouTube or similar platforms.

(h) Posting offensive, obscene or derogatory photographs, images, commentary or soundtracks on social and lifestyle websites.

(i) Transmitting or producing material which breaches confidentiality undertakings.

(j) Attempting to gain deliberate access to facilities or services which you are unauthorised to access.

(k) Deliberately undertaking activities that corrupt or destroy other users' data; disrupt the work of other users, or deny network resources to them; violate the privacy of other users; waste staff effort or networked resources.

(l) Creating or transmitting unsolicited commercial or advertising material unless that material is part of a service to which recipients have chosen to subscribe.

(m) Making commitments via email or the Internet on behalf of EP without full authority.

(n) Undertaking any activities detrimental to the reputation or business interests of EP.

(o)Attempting to gain deliberate access to facilities or services which you are unauthorised to access

(p) Deliberately undertaking activities that corrupt or destroy other users' data; disrupt the work of other users, or deny network resources to them; violate the privacy of other users; waste staff effort or networked resources

(q)Creating or transmitting unsolicited commercial or advertising material unless that material is part of a service to which recipients have chosen to subscribe

(r) Making commitments via email or the Internet on behalf of EP without full authority (s) Undertaking any activities detrimental to the reputation or business interests of EP

(t) Initiating or participating in the sending of chain letters, 'junk mail', 'spamming' or other similar mailings.

Users must take reasonable steps to safeguard all accounts, access credentials, and systems. EP reserves the right to investigate any activity that breaches this policy, including ICT misuse involving minors. Digital contact between staff and students under the age of 18 must take place only through official EP channels and must adhere to EP's Safeguarding and Prevent Policy.

Any user who inadvertently accesses an inappropriate Internet site must immediately close the session or return to the previous page. Any member of staff who receives an inappropriate email or message that appears to have been sent by another staff member or student should report the matter to the Chief Executive Officer or Managing Director.

Digital Safeguarding and Contact with Minors

Digital communication with students under the age of 18 must only be conducted through official EP platforms such as EP email or learning management systems. Staff must not use personal email accounts, messaging apps, or social media for direct communication with minors. Any concerns or breaches must be reported immediately in accordance with EP's Safeguarding and Prevent Policy.

Cybersecurity and Breach Management

All users must take reasonable steps to protect EP's ICT systems from unauthorised access, damage, or disruption. Passwords must be kept confidential and systems accessed only via authorised devices. Any suspected data breach, malware infection, or security incident must be reported immediately to the Head of School or ICT Manager. EP maintains a formal response protocol for investigating incidents and mitigating risks.

Computer crime and misuse

EP expects users to use ICT facilities, and in particular email and the Internet, responsibly at all times. Suspected computer crime and misuse of EP's ICT facilities, including excessive personal use by staff, will be investigated by the Managing Director and action taken accordingly. Staff are expected to complete mandatory ICT training on responsible use, reporting incidents and safeguarding, and refresher training at regular intervals.

Monitoring Use of EP ICT Facilities

Under the Telecommunications (Lawful Business Practice [LBP]) (Interception of Communications) Regulations 2000 (Statutory Instrument 2000 No.2699), EP reserves the right to monitor users' activities when using EP ICT and Wi-Fi facilities.

Monitoring may be carried out to:

- Record evidence of official transactions
- Ensure compliance with EP policies and regulatory requirements
- Maintain effective operation of systems (e.g., prevent viruses and service interruptions)
- Prevent or detect unauthorised use, misconduct, or criminal activity

In accordance with the Regulations, EP is required to inform users that such monitoring may take place. This policy document serves as one means of fulfilling that obligation.

Monitoring will always be proportionate and in accordance with relevant data protection legislation. EP maintains an ICT incident log and follows a formal breach response protocol. All concerns related to misuse or suspected breaches should be reported to the Head of School or ICT Manager without delay.

Incident Management Procedure

All suspected or confirmed ICT incidents, such as system misuse, unauthorised access, or disruption to services, must be reported promptly to the Head of ICT. An initial assessment will be undertaken to evaluate the impact and scope of the issue, followed by appropriate containment, investigation, and corrective action. A log of all ICT incidents and outcomes will be maintained for internal quality assurance and continuous improvement.

6. References and Related Policies

- EP Safeguarding Policies
- EP Student Disciplinary Policy and Procedure
- EP Staff Handbook
- EP Data Protection
- EP Privacy Policy

7. Forms

- ICT Incident Report Form

8. Policy Review

This policy will be reviewed annually by the Head of ICT in consultation with the Quality Assurance Committee, or earlier if significant regulatory or technological changes occur.

9. Appendices

- Appendix A: ICT Incident Reporting Form Template

This policy document was developed with the assistance of AI technology to support clarity, compliance, and alignment with international accreditation standards.

Appendix A – ICT Incident Reporting Form

English Path Incident Report Form.

For use by students and staff to report suspected or confirmed ICT-related incidents.

Section 1: Reporter Information

- **Full Name:** ______________________________
- **Role (Staff / Student):** ______________________
- **EP Campus:** ______________________________
- **Contact Email:** ____________________________
- **Contact Phone (if applicable):** _________________

Section 2: Incident Details

- **Date of Incident:** ____________________________
- **Time of Incident:** ____________________________
- **Location / Device Involved:** ____________________
- **Type of Incident (tick all that apply):**

☐ Unauthorised access or hacking

☐ Data breach or loss of data

☐ Malware or phishing attempt

☐ Inappropriate use of EP systems

☐ Inappropriate digital content or communication

☐ Violation of ICT Acceptable Use Agreement

☐ Other (please describe): ______________________

Section 3: Description of Incident

Please provide a detailed description of the incident. Include what happened, how it was discovered, any systems or data affected, and any immediate actions taken.

Section 4: Supporting Evidence

List or attach any relevant files, screenshots, emails, or logs that support this report.

Section 5: Reporter Declaration

I confirm that the information provided in this form is accurate to the best of my knowledge and understand that the incident will be investigated according to EP policy.

- **Signature:** ______________________________ **Date:** __________________________________

Submission Instructions

Once completed, please submit this form to the **Head of School** or the **ICT Manager** at your EP campus. If the incident involves a safeguarding concern or a student under 18, it must also be reported to the **Designated Safeguarding Lead (DSL)** in accordance with the **EP Safeguarding Policy**.