Acceptable Use Policy

Policy Dated:	July 2025
Adopted by Full Board	July 2025
Date of Next Review:	July 2027
Reason for Review/Revision:	As per policy review schedule Update from PHP Law re. personal devices
Publication Scheme	Trust & School websites
Version	05
Lead	CEO

Section 1

1.1 Introduction

This policy aims to clearly define what is and is not acceptable and how unacceptable use will be dealt with. The policy deals specifically with internet use but should be read in conjunction with all information security related policies.

The objectives of the Internet Acceptable Use Policy are set out in Section 2. However, as a general rule all Extol staff should at all times conduct themselves honestly and appropriately when using internet facilities, and in particular must not:

- place at risk the confidentiality, integrity or availability of either Extol's or any school's information, information systems or equipment
- engage in any action or activity which would make yourself as individuals the trust or any school liable to criminal prosecution or civil action
- create an unauthorised contractual liability on the part of Extol or any school
- access or disseminate any inappropriate material
- create, access or disseminate any offensive material, including but not limited to material of a racial, sexually explicit, discriminatory or defamatory nature
- engage in any activity that would bring Extol Trust or any schools within the partnership into disrepute

1.2 Policy Review

The Trustees of Extol Trust will review and evaluate the effectiveness of this policy. The policy may be withdrawn or amended in accordance with information security policy review procedures. Staff are encouraged to feedback any comments or issues encountered when operating the policy in practice.

1.3 Scope

This policy applies to **all** employees including:

- those in full time or part time employment on fixed term or permanent contracts with Extol
- those employees on secondment (subject to terms and conditions of the secondment arrangement)
- agency and casual staff (this includes volunteers)
- consultants, contractors and third party suppliers (where applicable)

For the purpose of this policy all of the above are referred to as "staff". However, this term is not intended to determine employee status.

This policy applies to any facilities provided by Extol or the schools for internet access whether working on Extol or school premises or making use of equipment at home or in any premises such as hotels and conference venues.

Although it is not intended to unduly impact on the private use of the internet from non-school facilities, those parts of this policy relating to the posting of unauthorised material or opinions on the internet in a manner that can be attributed to a member of staff apply whether from official facilities, facilities provided by third parties or facilities under the control of members of staff.

Awareness of this policy should be included in all induction training for new staff and should be included as appropriate on refresher training courses to existing staff.

Copies of this and other information security policies and guidelines will be published on SharePoint and on Extol's website.

1.4 Data Protection & GDPR

Extol Trust is fully committed to compliance with the Data Protection Act 2108 and the UK GDPR. In order to effectively carry out its business Extol must collect and use information on staff internet usage. All information collected will be processed in accordance with the principles of the Acts.

Section 2 - Internet Acceptable Use Policy

2.1 Objective

The use of the internet by staff is permitted and encouraged where such use supports the goals and objectives of the business. In accessing the internet staff must ensure that they:

- comply with current legislation
- use the internet in an acceptable way
- do not create unnecessary business risk to Extol or to schools by their misuse of the internet

2.2 Policy Statements

Access to the internet is permitted for legitimate business purposes and limited personal use subject to management discretion and acceptable and proper use. Acceptable use is defined in Section 3.

Deliberate access or attempted access to inappropriate sites is strictly forbidden and could lead to disciplinary action up to and including dismissal.

Access to the internet and other ICT services is made available to staff and not to visitors, except by prior authorisation by a senior member of Extol or school staff.

Personal use of internet facilities is allowed for staff as long as it is within established parameters (see Section 3) and is in their own time (for example lunch time, or at the start and end of the day when staff are 'clocked out').

Personal use is not a right, it is a facility given at the discretion of management and may be withdrawn at any time for operational reasons, or where abuse is suspected or detected.

Staff must not enter into official contracts or financial commitments on behalf of Extol or the schools in our partnership without proper authorisation in accordance with formal procurement procedures.

Access to the internet will be controlled by an appropriate software filtering solution configured to prevent accidental or deliberate navigation to inappropriate websites.

2.3 Roles and Responsibilities

This policy is owned by Extol Trust and is provided by the CEO. All staff are responsible for ensuring that they comply with the policy and associated guidance.

Section 3 – Personal Device Acceptable Use Policy

3.1 Extol Trust recognise that many staff choose to access information from their own devices.

Any member of staff wishing to do this must be aware that they have a direct personal responsibility for ensuring that the device they choose to use has the benefit of encryption, that is above and beyond a simple password protection.

Staff must ensure that personal devices such as mobile smart phones, tablets and other portable electronic equipment are set to lock and only open with encrypted passcodes to prevent unauthorised access.

The Trust will support and enable staff to ensure that their devices are compliant.

If any member of staff uses a device without these safeguards in place it will be a disciplinary breach if data is unlawfully accessed by a third party.

Encryption protection will be available for staff and suitable advice provided.

Section 4 - Guidance

3.1 Access

Extol uses Securly filtering and monitoring provided by our service provider OneIT across its network which is designed to prevent accidental or deliberate access to inappropriate sites by clients or staff. The software categorises websites and access is controlled by allowing or blocking certain categories (for example access to the 'sexual material' category is blocked). There are occasions where Extol staff will have legitimate business reasons to by-pass the filtering or to access websites that are members of 'blocked' categories. In such cases permission will be granted to by-pass the filtering or to allow access to specific websites by a senior member of Extol or school staff and where necessary the request logged.

3.2 Monitoring

All internet access is logged and can be monitored to ensure compliance with the policy. Any inappropriate internet access which is identified will be reported to the Head of the individual school or the CEO of Extol and investigated. In accordance with Extol's legal duty

any access to or downloading of illegal material (for example, child pornography) will be reported to the police.

3.3 Acceptable Use

Due to the nature of the internet and the diverse requirements of staff it is not possible to set out definitively what is or is not acceptable use. In general staff are considered capable of recognising sites which contain inappropriate material.

3.4 Unacceptable Use

Unacceptable use will always be a matter of considering all the circumstances of an individual case, but in the absence of specific authorisation from Extol or school senior management following is considered as unacceptable use or behaviour.

- deliberate access or attempted access to sites that contain obscene, racist, hateful or pornographic material
- deliberate access or attempted access to sites that contain violence, weapons or terrorism material
- deliberate access or attempted access to gaming and gambling sites
- using internet facilities to send or publish offensive, defamatory or harassing material (for example via social networking sites such as Facebook)
- using internet facilities to perpetrate a fraud (for example software or music piracy)
- unauthorised downloading of software or video and music files
- unauthorised downloading of copyright material
- deliberate internet activities that waste staff time or network resources
- the introduction of any form of malicious software
- using facilities such as messaging services, chat rooms or blogs in any manner that could bring the school, its staff or governors into disrepute
- disclosing or attempting to disclose any information that is not in the public domain

3.5 Breach of Policy

It is not the intention of Extol to penalise anyone for a genuine mistake. Accidental breaches of policy will be recorded and the circumstances investigated in order to identify if there are any improvements that can be made to prevent a recurrence, and staff are encouraged to report such incidents.

Failure to comply with this policy and associated guidance may lead to disciplinary action being taken against staff up to and including dismissal. Breaches may also result in legal action taken against individual staff.

3.6 Advice and Further Guidance

Questions relating to any aspect of this policy should be raised with the individual Headteachers or CEO.