

IT Acceptable Use Policy

Contents

Contents	2
1.0 Introduction	3
1.1 Purpose of [policy]	3
2.0 Policy	3
2.1 Process	7
Auditing	7
Contact Us	8

1.0 Introduction

This Acceptable Usage Policy is guidance for staff and students and covers the security and use of all BCNO Group information systems and IT equipment.

It is the responsibility of every student and staff member or contractor to follow these guidelines and to conduct their activities accordingly.

It also includes the use of email, internet, voice and mobile IT equipment.

1.1 Purpose of [policy]

The purpose of this policy is to outline the acceptable use of computer equipment and systems at the BCNO Group. Inappropriate use exposes the BCNO Group to risks including virus attacks, compromise of network systems and services, and legal issues.

2.0 Policy

The policy sets out and defines what is expected of its IT users and what is deemed acceptable when using BCNO Group IT systems.

Access to all BCNO Group IT systems is controlled by the use of User IDs and passwords, all User IDs are uniquely assigned to an individual and consequently individuals are accountable for use of their account.

Users must not:

- Allow anyone else to use their user ID to access any BCNO Group system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access BCNO Group systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to IT systems or information, including changes to settings, the installation or removal of software and alterations to

hardware or connectivity.

- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Connect any non-authorised device to the BCNO Group network or IT systems without prior permission from the IT Leads.
- Store BCNO Group data on any non-authorised equipment.
- Give or transfer BCNO Group data or software to any person or organisation outside without the authority of the IT Leads.

Internet and email Conditions of Use

The BCNO Group has a duty of care to filter all web content to ensure its users are protected against unsuitable content including but not limited to adult material, gambling, drugs, offensive, hate, discrimination, racism, violence, terrorism, and extremism, attempting to access or bypass filtering to access this content will be deemed as unacceptable use for which users will be subject to BCNO Group disciplinary procedures.

Use of the BCNO Group internet and email is intended for school business, study and research. Occasional moderate personal use is permitted where such use does not affect the individual's business/learning performance, is not detrimental to the BCNO Group in any way, does not breach any term and condition of employment or learner agreement and does not place the individual or the BCNO Group in breach of statutory or other legal obligations. All individuals are accountable for their actions on the internet and email systems.

Users must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use the internet or email to access or share any material that may be considered

to relate to terrorism or extremism, nor should such material be downloaded or stored on systems owned or controlled by the BCNO Group.

- Use the internet or email to engage in or support the radicalisation or potential radicalisation of any individual, whether that person(s), known or unknown are within the BCNO Group or not.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which the BCNO Group considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to the BCNO Group alter any information about it, or express any opinion about the school, unless they are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally.
- Make official commitments through the internet or email on behalf of the BCNO Group unless authorised to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.

Monitoring and Filtering

All internet access is filtered and monitored. Audits and logs from other IT systems will be checked where appropriate. Investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. The BCNO Group has the right to monitor activity on its systems, including internet and email use, to ensure systems security and effective operation, individual performance and to protect against misuse.

Any attempted breaches are automatically reported to the Information technology team, detailing the attempted violation and the number of times attempted. A technology team lead will review reports and any reports which contain multiple attempts to access restricted content will be reported to the relevant faculty or department manager.

Our firewall software ESET Smart Security, may, for security reasons, automatically prevent your browser from accessing specific websites or even domains. This is due to the risks related to traffic originating from these websites/domains. The risk assessment is based on several criteria. The most important parameter in evaluating the potential risk is the amount of malicious traffic originating from a specific website/domain.

If a website has been blocked by your ESET product, one of the following warnings will be displayed in your browser window (depending on what version you have installed):

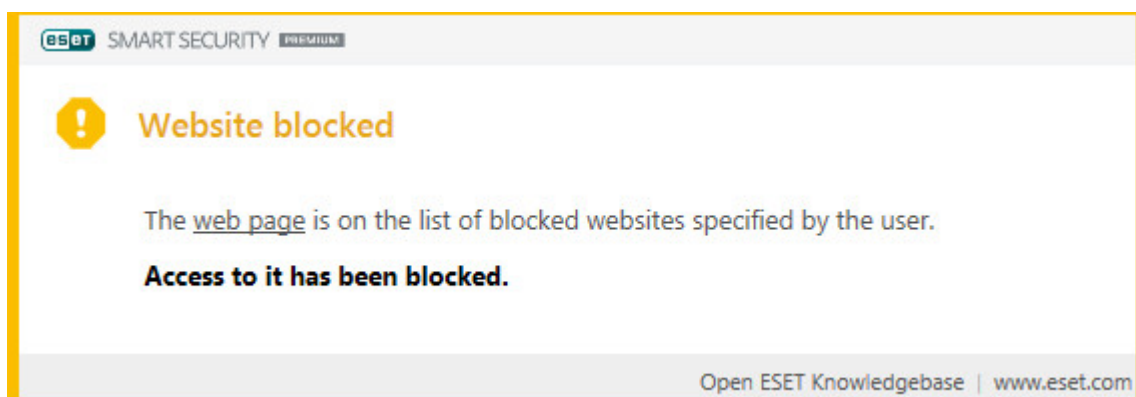


Figure 1-1

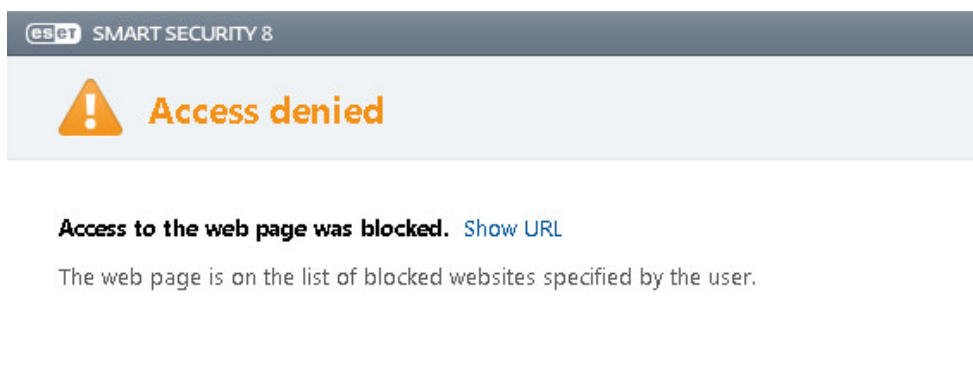


Figure 1-2

If access to your website/domain has been blocked and you know this preventive measure performed by the ESET product to be a false positive, please report this to either IT leads, who will report this to

our IT support contractor and ask they log this and allow access.

Enforcement

Failure to adhere to this policy may result in disciplinary action which could include termination of employment.

Key Relevant Documents

IT Policy

Email Policy

Password Policy

Data Protection Policy

Prevent Policy

2.1 Process

Step	Process	Role Holder Responsible
1	Ensure staff and students are aware of this policy and any updated versions	Info Services Manager Kent/ Facilities Manager London
2	To abide by this policy	All students and staff
3	Ensure the ESO systems are filtered robustly to ensure that any unsuitable material found is traced, filtered and blocked.	Info Services Manager Kent/ Facilities Manager London
4	Review and monitor reports generated by IT systems	Info Services Manager Kent/ Facilities Manager London
5	Disciplinary actions resulting from enforcement of policy	Registry /Head of HR

Auditing

Policy Name:	IT Acceptable Use Policy
Policy Owner:	Information Services Manager Kent /Facilities Manager London

Policy Approver:	Senior Management Team		
Audience:	Employees, students and visitors		
Storage Location:	VLE – Learning Zone / Microsoft Teams/Website		
Effective Date:	01.2023		
Review Date: (Unless other revisions are required prior to this date)	10.2026		
Version:	V1.2		
Equality Impact Assessment:	Are there any implications for a protected characteristic group as defined by the Equality Act 2010 in this policy?		
	<input type="checkbox"/> Positive Impact	<input type="checkbox"/> Negative Impact	<input checked="" type="checkbox"/> Neutral
Details:			

Contact Us

Library & Information Services Manager – Kent

Sarah Hunter

E: Sarah.Hunter@bcnogroup.ac.uk

European School of Osteopathy

104 Tonbridge Road

Maidstone

Kent ME16 8SL

+44 (0)1622 671558

Version History

Version	Date	Action	By
1.0	Jan 2023	Rebranding	SH
1.1	July 2024	Annual Review	SH
1.2	Oct 2025	Annual Review	SH