STOKE ON TRENT COLLEGE	**POLICY 55** **ACCEPTABLE USE POLICY**	European Union European Social Fund Investing in jobs and skills

1. Purpose, Scope and Users

The purpose of this policy is to define clear rules for the use of information systems and other information assets at Stoke on Trent College.

Users of this policy are all employees, students and visitors at Stoke on Trent College.

1.1 Staff

College staff to comply with the provisions of this Acceptable Use Policy (AUP) either by signing an electronic version of the AUP or by physical signature on a copy of this AUP. Staff are also informed of their obligations when logging onto College devices or using the Staff BYOD network. Staff connect to the Staff BYOD network on the understanding their network traffic is monitored for adherence to web filtering and safeguarding policies but is not intercepted and analysed e.g. passwords to external services cannot be identified.

1.2 Student

A student confirms acceptance of this AUP by enrolling with the College; once a student enrolment is confirmed, user privileges are conferred and compliance with this AUP will be required. Students are informed of their obligations when they are supplied with their network account and when logging onto College devices or using the Student BYOD network. Students connect to the Student BYOD network on the understanding their network traffic is monitored for adherence to web filtering and safeguarding policies but is not intercepted and analysed e.g. passwords to external services cannot be identified.

1.3 Visitors

A visitor is responsible for the security and maintenance of their own device whilst located within the College estate. Connection to the guest or BYOD is provided on the understanding that the following policy also applies to the use of data on those networks with regards to network traffic, unacceptable material and the control of usernames and passwords. Visitors connect on the understanding their network traffic is monitored for adherence to web filtering and safeguarding policies but is not intercepted and analysed e.g. passwords to external services cannot be identified.

2. Acceptable Use of Information Assets

2.1 Definitions

Information system – includes all servers and clients, network infrastructure, system and application software, data, and other computer sub-systems and components, which are owned or used by the organisation or which are under the organisation's responsibility. The use of an information system also includes the use of all internal or external services, such as Internet access, e-mail, etc.

Information assets – in the context of this policy, the term *information assets* are applied to information systems and other information/equipment, including paper documents, mobile phones, portable computers, data storage media, etc.

2.2 Acceptable Use

Information assets used only for business needs with the purpose of executing College-related tasks.

2.3 Responsibility for Asset

Each information asset has an owner designated in the Inventory of Assets. The asset owner is responsible for the confidentiality, integrity and availability of information in the asset in question.

Prohibited Activities

It is prohibited to use information assets in a manner that unnecessarily takes up capacity, weakens the performance of the information system or poses a security threat. It is also prohibited:

- To download image or video files which do not have a business purpose e.g. send e-mail chain letters, play games, utilise personal media files
- Install software on a local computer without explicit permission from IT Services.
- To use portable software that does not require installation and can operate under non-elevated privileges.
- To use private VPN applications and services for any reason without authorisation by the Director of IT and Digital.
- To reroute or encrypt network traffic for the purposes of evading web filtering, identification and security control operations.
- To use Java applications, Active X controls and other mobile code, except when authorised by the Director of IT and Digital.

- To use cryptographic tools on a local computer.
- To download and/or execute program code from external media.
- To wirelessly transmit data to other devices without prior agreement e.g. AirDrop images to College devices without explicit permission from the controller of the device.

3. Taking Assets Off-Site

IT equipment regardless of its form or storage medium, may not be taken off-site without prior authorisation by the IT and Digital Team, excluding laptops issued to staff members.

As long as said assets are outside the College, they have to be controlled by the person who was granted permission for their removal.

4. Return of Assets Upon Termination of Contract

Upon termination of an employment contract the user must return all IT and IT-related equipment to IT and Digital. In the event that this is not possible, the line manager of the outgoing employee is responsible for the return of all equipment.

5. Anti-Virus Protection

Sophos must be installed on every College PC and College-issued smart phone with activated automatic updates, this is controlled and managed by IT and Digital.

6. Authorisation for Information System Use

Users of information systems may only access those information system assets for which they have been explicitly authorised by the asset owner.

Users may use the information system only for purposes for which they have been authorised i.e. for which they have been granted access rights.

Users must not take part in activities which may be used to bypass information system security controls.

User access is monitored and profiled for performance and security logging purposes.

7. User Account Responsibilities

The user must not directly or indirectly allow another person to use his/her access rights e.g. must not use another person's username and/or password. Users must not impersonate another user for any reason. Email delegation must only take place under specific authorised circumstances by the manager of the department. The use of group user names is forbidden; generic email addresses can be utilised but are subject to the same conditions as a user with a nominated account user who will be held ultimately responsible for all activity on that email address.

The owner of the user account is its user, who is responsible for its use, and all transactions performed through this user account. Transactions are logged and audited.

8. Password responsibilities

Users must apply good security practices when selecting and using passwords:

- Passwords must not be disclosed to other persons, including management and system administrators.
- Passwords must not be written down.
- User-generated passwords must not be distributed through any channel (using oral, written or electronic distribution, etc.).
- Passwords must be changed if there are indications that the passwords or the system may have been compromised – in that case a security incident must be reported to the Data Protection Officer.
- Strong passwords must be selected, in the following way:
    - Using at least eight characters.
    - Using at least one numeric character.
    - Using at least one uppercase and at least one lowercase alphabetic character.
    - Using at least one special character.
- A password must not be a dictionary word, dialectal or jargon word from any language, or any of these words written backwards.
- Passwords must not be based on personal data (e.g. date of birth, address, name of family member, etc.)
- The last three passwords must not be re-used.
- Passwords must be changed every 3 months.
- Passwords must be changed at first log-on to a system.
- Passwords must not be stored in an automated log-on system (e.g. macro or browser) with the following exceptions:

- Some College IT services are provided with a Single Sign On facility where the Microsoft 365 password is shared between services.
- If a browser's saved passwords function is used, the retrieval of those passwords must be protected by a further credential requirement to unlock or view those passwords.

- Passwords used for private purposes must not be used for business purposes.

9. Clear Desk and Clear Screen Policy

- No confidential, commercially sensitive or personally identifiable information should be left unattended on desks through either manually locking workstations or locking physical media away.
- When operating in an open-plan or public environment, screen privacy filters should be used where necessary when utilising sensitive information to restrict the view of the screen to the person using the screen.

All information classified as "Internal use," "Restricted" and "Confidential" as specified in Policy 56 Data Classification Policy are regarded as sensitive in this item.

9.1 Clear Desk Policy

If the authorised person is not at his/her workplace, all paper documents, as well as data storage media labelled as sensitive, must be removed from the desk or other places (printers, fax machines, photocopiers, etc.) to prevent unauthorised access.

Such documents and media must be stored in a secure manner in accordance with the Data Classification Policy.

9.2 Clear Screen Policy

If the authorised person is not at his/her workplace, all sensitive information must be removed from the screen, and access must be denied to all systems for which the person has authorisation.

In the case of short absence (up to 30 minutes), the clear screen policy is implemented by logging out of all systems or locking the screen with a password. If the person is absent for a longer period of time, the clear screen policy is implemented by logging out of all systems and turning off the workstation.

All Staff members are required to log off and shut down their workstation at end of each day.

10. Protection of Shared Facilities and Equipment

Documents containing sensitive information must immediately be removed from printers, fax and copy machines.

Unauthorised use of printers, photocopiers, scanners and other shared equipment for copying is prevented by access cards.

11. Internet Use

Internet is accessed only through the College local network howsoever joined with appropriate infrastructure and firewall protection. The College internet access is provided via the JISC-operated JANET National network. While using the internet, all users must agree to the JANET Acceptable Use Policy[1].

IT may block access to some internet pages for individual users, groups of users or all employees at the College. If access to some web pages is blocked, the user may submit an IT helpdesk request to access such pages to seek authorisation from the Director of IT and Digital who may refer the request to senior management at the College for consideration. The user must not try to bypass such restriction autonomously.

The user must regard information received through unverified websites as unreliable. Such information may be used for business purposes only after its authenticity and correctness have been verified.

The use of Peer to Peer software, including Bittorrent, qBittorrent, Vuze and Deluge, access to the "Dark Web" or Tor Networks is not permitted to run while connected to College networks. Any VPN software including ExpressVPN, OpenVPN, PortableVPN or any web-based VPN that is not provided by IT and Digital is not permitted.

The user is responsible for all possible consequences arising from unauthorised or inappropriate use of internet services or content which may include disciplinary procedures.

Misuse of College internet access or any attempt to circumvent security systems, including web filtering, will result in disciplinary or legal action.

[1] https://community.jisc.ac.uk/library/acceptable-use-policy

12. E-mail and Other Message Exchange Methods

Message exchange methods, other than electronic mail, also include download of files from the internet, transfer of data, telephones, fax machines, sending SMS text messages, portable media, forums and social networks.

Users may only send messages containing true information. It is forbidden to send materials with disturbing, unpleasant, sexually explicit, rude, slanderous or any other unacceptable or illegal content. Users must not send spam messages to persons with whom no business relationship has been established or to persons who did not require such information.

Should a user receive a spam e-mail, he/she must inform IT and Digital.

The user must save each message containing data significant for the College business using the method specified.

Each e-mail message must contain a disclaimer, except messages sent through communication systems determined by IT.

13. Copyright

Users must not make unauthorised copies of software owned by the College, except in cases permitted by law, by the owner or IT.

Users must not copy software or other original materials from other sources, and are liable for all consequences that could arise under the intellectual property law.

When copying information assets for legitimate teaching and learning purposes through the College's multi-function devices, the use of Copyright Licensing Agency functionality must be used to provide a digital copy of all materials via the CLA integration module to the copyright authorities.

14. Mobile Computing

14.1 Introduction

Mobile computing equipment includes all kinds of portable computers, mobile phones, smart phones, memory cards and other mobile equipment used for storage, processing and transferring of data.

14.2 Basic Rules

Special care should be taken when mobile computing equipment is placed in cars or other forms of transportation, public spaces, hotel rooms, meeting places, conference centres, and other unprotected areas outside the College premises.

The person taking mobile computing equipment off-premises must follow these rules:

- Mobile computing equipment carrying important, sensitive or critical information must not be left unattended and, if possible, should be physically locked away, or special locks should be used to secure the equipment.
- When using mobile computing equipment in public places, the user must take care that data cannot be read by unauthorised persons or screens overlooked.
- Updates of patches and other system settings are performed.
- Protection against malicious code is installed and updated.
- The person using mobile computing equipment off-premises is responsible for regular backups of data.
- Connecting to communication networks and data exchange must reflect the sensitivity of data and is performed with prior acknowledgement of the network's security risk being identified e.g. access to public Wi-Fi networks is usually not encrypted and as such sensitive data must not be transmitted.
- Protection of sensitive data must be implemented.
- In case mobile computing equipment is left unattended, rules for unattended user equipment must be applied in line with the Clear Desk and Clear Screen Policy.

15. Safeguarding and Prevent

The following activity is actively monitored and logged as part of the College's responsibility towards multi-agency safeguarding and PREVENT agendas.

- Information which may lead to potential terrorism or extremist activity.
- Internet activity including sites categorised as:
    - Intolerance
    - Personal Weapons
    - Terrorism
    - Violence
- Information which may lead to a potential risk to young people or vulnerable adults.
- Internet activity including sites categorised as:
    - Adult Entertainers/Entertainment

- Adult Sites
- Child Abuse
- Pornography
- Material restricted to Adults

Logs and information relating to Safeguarding or PREVENT will be shared with the College's trained Safeguarding/Prevent officer and may be shared with local authorities for further investigation.

16. Monitoring of Information and Communication Systems

The College records and monitors the use of its IT facilities, under the Regulation of Investigatory Powers Act (2000)[2] for the purposes of investigation, detection and prevention of infringement of the law and investigation of alleged misconduct by staff or students. User behaviour is profiled and monitored for the identification of unusual or unexpected behaviour to assist with early identification of cryptoware or ransomware which involves an unusually high amount of activity within a short timeframe.

All data which is created, stored, sent or received through the information systems or other College communication systems, including various applications, e-mail, Internet, fax, etc., whether it is personal or not, is considered the ownership of Stoke on Trent College.

Users agree that authorised persons from the College may access all such data, and that access by such persons will not be considered a violation of the users' privacy.

The College may use specialised tools for the purpose of identifying and blocking forbidden methods of communication and filtering forbidden content.

17. Approval

Approved by the College Executive Team

Signed:

[2] https://www.legislation.gov.uk/ukpga/2000/23/contents

(Principal)

Endorsed by the College Corporation

Signed:

(Chair)

Issued	Reviewed						
13/05/20	04/12/22						