IT Acceptable Use Policy

Document Created	01/02/2010
Date of Last Revision	05/04/2022
Date of Impact Assessment	05/04/2022
Version No.	11
Author	Burhan Loqueman
Approved by	BMSG
Associated Policies	IT Cyber Security Policy

a a A n ool

a o ol
A a ol

Y o

The purpose of this document is to ensure that all users of Suffolk New College computing facilities, including employees, students, visitors, partners and contractors are aware of the organisation's policies relating to their use.

Proper use of information technology is fundamental to the reputation and operational effectiveness of Suffolk New College. However, any abuse of computing facilities - in particular e-mail and internet access - may expose Suffolk New College and individuals to legal and criminal liability, potential financial loss and damage to reputation.

Suffolk New College encourages the use of computing facilities for the mutual benefit of the organisation, employees and learners. Similarly, the regulations that constitute this policy seek to provide for the mutual protection of Suffolk New College and the rights of its employees and learners.

Suffolk New College also has the right to determine whether any activity, though legal, is still unacceptable within the context of a high-quality education and skills provider that serves as responsible member of the local community, trusted by both parents and sponsors of learners.

It is therefore critical that all users read and understand this document and make themselves aware of the risks and exposure involved. It is the responsibility of all users of Suffolk New College computing facilities to follow all IT and related policies and to seek advice in case of doubt.

A

It is important to highlight related policies and codes of conduct that the College has in place which this policy supports at a technical level as well as where specific policies and guidelines cover both technical and non-technical areas. All these policies can be found on the staff intranet.

These include:

- The Code of Conduct
- The eSafety Policy
- The Social Media Policy
- The Data Protection Policy
- The IT Cyber Security Policy

This policy may be updated or supplemented by specific standards or procedures to reflect further developments in technology or legislation or other relevant changes.

More detailed policies regarding sections of this overall policy may also be found on the staff intranet.

? A

?

The phrase ‘Computing Facilities’ as used in this policy shall be interpreted as including any computer hardware or software owned or operated by Suffolk New College and any allocation of time, memory, disk space or other measure of resource on any of Suffolk New College’s hardware, software or networks. This definition can also be expanded to include services, software and hardware used by the College but hosted elsewhere, for example Cloud services such as Google Workspace, Microsoft 365 and outsourced database systems and services.

?? A A A A A ABA

?

Authorisation

The process by which a party obtains their right of access to any given service or information.

Access

The process by which a party uses a service or information source for which they have been authorised.

Privilege

The level and scale of changes, control and editing/amendments that a party is permitted with respect to information or a service.

Role

A categorisation process of all individuals that in some way use services or information owned or operated by Suffolk New College. Users with the same role would by definition within a role-based security framework automatically qualify for set levels of *authorisation*, *access* and *privilege*.

However, assignment to the full set of privileges, and access associated with a role will normally be conditional on completion of training, additional vetting, probationary periods, etc., as managed by the authorising party.

? A

Authorisation for the use of any of Suffolk New College’s computing facilities is ultimately at the discretion of Executive Management Team and handled operationally by line and departmental managers, whilst *access* to most computing facilities was traditionally managed by IT Services.

Those facilities and systems that have within them varying levels of database access/rights i.e. *privileges* are controlled by the departmental managers responsible for those systems.

Increasing use of cloud-based and online services hosted outside of the College also now means that departmental managers and their staff have more autonomous control and therefore responsibility over granting of access rights to systems, services and data.

?

Computing facilities owned by Suffolk New College and software and/or data developed or created (for whatever reason) on that equipment remains in all respects the property of Suffolk New College. This also extends to systems operating in the Cloud or offsite. The Patents Act 1977 and the Copyright, Designs and Patents Act 1988 provide for the Intellectual Property Rights (IPR) in that work created by an employee in the course of his/her employment is vested automatically to the employer.

? A A

Desktop PCs are a critical asset to Suffolk New College and must be managed carefully to maintain security, data integrity and efficiency.

All users have access to appropriate areas on Suffolk New College's file servers for the secure storage of valuable files. Valued documents and files should not be stored on Desktop PCs (for example the drive C or D). Files stored on Desktop PCs are at risk of loss through hardware/software failure or automated administrative activity. IT Services shall take no responsibility for the support or recovery of data lost when it is stored in any location other than central server systems.

Desktop PCs are asset-managed components and are subject to asset and change control. Users must contact IT Services in order to request any change in location of configuration of these assets. This includes making any changes to layout, movement of PCs, etc.

Keyboards, mice and currently monitors, though not asset controlled, shall not be changed or removed.

? A AB A A A AB

Laptop PCs are at high risk from loss or theft and require additional security protection. All reasonable precautions must be taken to ensure that hardware is stored securely. Also, to protect the integrity of Suffolk New College systems and data procedures, passwords used to gain access to Suffolk New

College systems must not be stored with the computer. This includes the saving of passwords into remote access software.

If your Laptop PC is lost or stolen IT Services must be notified as soon as possible and a report made to the police.

Further information regarding laptops can be found in the IT Services Laptop Support Policy.

? B

Handhelds and mobiles are at high risk from theft due to their size and nature of usage.

Staff should take care to keep these devices concealed when not in use and to be conscious of onlookers who may be targeting devices for theft. In the

? A

Policy regarding loan equipment is similar to that for laptops and handheld or mobile devices. Most loan equipment is highly portable and attractive to thieves. Users who borrow loan equipment shall sign for it and bear the responsibility for its care. Loan equipment should be concealed and stored securely when not in use.

If loan equipment is stolen or lost, IT Services should be informed immediately. It may also be that the user responsible for its care has to report the theft to the police and report the incident number to IT Services.

? A

staff using older devices are required to check which version of Windows or Mac OS, IOS or Android they have on their mobile phone.

If IT Services are given this information we can help check to see if the computer is still supportable and safe to use.

? A A A

Only software properly purchased and/or approved by IT Services may be used on College computers.

Unauthorised installation of any software or apps on computers and laptops owned by the College is prohibited.

Only IT Services personnel may install any software. For clarification of a machine's status as a 'managed Desktop PC' please consult IT Services.

Mobile devices will also fall into this category as we develop our mobile management platform capabilities, however, we have made allowances for staff to install apps in the past due to the need for flexibility and speed of access to key apps.

Whilst it is the user's responsibility to take reasonable care when using their computer hardware, specifically laptops, it is possible for software to be installed on a machine without the full comprehension of the user. Users discovering software that has been installed in an unsolicited manner and which contravenes the licensing regulations above must contact IT Services who may assist in resolving any issues including the removal of such software, which may well pose a security risk.

Further information about software support may be found in the IT Services Software Support Policy.

? ? A A Y

You must only access information held on Suffolk New College's computer systems if you have been properly authorised to do so and you need the information to carry out your work.

Currently, authorisation is provided to IT Services by your line manager, with ultimate responsibility for authorisation resting with the Executive Management Team.

Under no circumstances should you disclose personal or other confidential information held on computer to unauthorised persons. The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computers' Misuse Act 1990.

It is corporate policy to store data on a network drive where it is regularly backed up, whilst IT Services accepts no responsibility for data stored on external media such as USB memory sticks.

Anti-virus software must not be removed or deactivated, nor any attempt made to interfere or bypass anti-virus functions. Files attachments received or sent by e-mail via the internet are scanned for viruses automatically by our email systems.

Users must not intentionally access or transmit computer viruses or indeed software or programs of any type.

Non-Suffolk New College software or data files intended to be run on corporate equipment by external persons such as engineers or trainers must be scanned for viruses before use by IT Services. If you suspect that a virus has infected a computer then stop using the computer, switch it off, and contact IT Services immediately.

Further information about Anti-Virus protection may be found in the IT Services Anti-Virus and Anti-Malware Support Policy.

? A Y

Passwords protect Suffolk New College systems from access by unauthorised people: they protect your work and the organisation's information. Therefore, never give your network password to anyone else. Passwords are of a minimum length and old passwords cannot be re-used immediately – the last 3 passwords used will not be re-usable.

Passwords must be 10 or more characters long with both upper and lower case characters, numbers and non-standard characters such as an exclamation mark.

However, we strongly recommend all staff and students to adopt longer 'pass-phrases' consisting of multiple words concatenated without spaces, with random spelling errors, and mixture of upper/lower case characters, numbers and symbols. At this time, 15 characters is the recommended length however the College password policy allows for 10 characters to be used to facilitate learners.

Further information about password security may be found in the IT Services Password Policy.

? A Y

Suffolk New College does not currently allow the connection of non-corporate computer equipment to the wired network without prior request and technical approval by IT Services – and this is typically only allowed for contractors, auditors and other authorised parties that the College has operational business or curriculum purposes to fulfil.

Any wireless network access will be subject to acceptable usage policy with additional guidelines on safety and security.

For further information, please see the IT Services Network Access Security Policy.

Suffolk New College's IT policies are available on the staff intranet. Please read those in conjunction with this document as it integral to the acceptable use of IT at Suffolk New College.

A A

Suffolk New College users must ensure prior approval at Executive Management Team before attempting to:

1. Obtain clearance to create websites on Suffolk New College computing

A

A B Y

Suffolk New College’s e-mail system is provided for the organisation’s business and curriculum purposes. E-mail is now a critical business tool but inappropriate use can expose Suffolk New College and the user to significant liability. Liability can arise in a number of ways including, among others, phishing and ransomware/malware attacks, credential theft, copyright or trademark infringement, misuse of confidential information, defamation and liability for inaccurate statements and breaches of personal information/email addresses.

The e-mail system has an associated resource and finance cost and it must be used judiciously in the same manner as other organisational resources.

Corporate-wide e-mail messages must be business related and of significant importance to all employees, and as such subject to Executive Management Team approval. College staff wishing to communicate to all staff in this manner must pass such messages onto their relevant line manager.

It is expressly forbidden for any staff member to seek to avoid this obligation by sending emails individually to multiple members of staff or to attempt to select all staff on the email address list.

?

E-mail messages must be treated like any other formal written communication.

E-mail messages cannot be considered to be private, secure or temporary when in transit and the text and attachments will be scanned by anti-spam and anti-virus systems.

Although encryption is employed where possible, not all email destinations across the internet fully support encryption for sending and receiving email. Therefore staff should NOT assume that emails cannot be read by third party email processing systems.

Email can be copied and forwarded to numerous recipients quickly and easily and you should assume that they could be read by anyone.

Improper statements in e-mail can give rise to personal liability and liability for Suffolk New College and can constitute a serious disciplinary matter. E-mails that embarrass misrepresent or convey an unjust or unfavourable impression of Suffolk New College or its business affairs, employees, suppliers, customers or competitors are not permitted.

Do not create or send e-mail messages that are defamatory. Defamatory e-mails whether internal or external can constitute a published libel and are actionable. Never send confidential or sensitive information via e-mail. E-mail messages, however confidential or damaging, may have to be disclosed in court proceedings.

Do not create or send e-mail messages that may be intimidating, incite hatred, encourage or condone acts of terrorism, drug-abuse, are hostile or offensive on the basis of sex, race, colour, religion/culture, national or regional origin, sexual orientation/identification or disability.

It is never permissible to subject another employee to public humiliation, harassment or ridicule; this is equally true via e-mail.

Copyright law applies to e-mail. Do not use e-mail to transmit or circulate copyrighted materials.

A Y

A

The laws of all nation states regulating such diverse subjects as intellectual property, fraud, defamation, pornography, insurance, banking, financial services and tax apply equally to on-line activities. However, the practical legal position regarding Internet usage is often uncertain.

Strictly, documents must not be published on the web which are defamatory or which may constitute intimidating, incitement to hatred or terrorism, drug-abuse, hostile or offensive material on the basis of sex, race, colour, Postings to newsgroups, chat rooms and forums and social networking sites are in effect e-mails published to the world at large and are subject to the same regulations governing email as above.

meeting software. Never attempt to install or download software on your own.

c) Personal use of web and video/audio conferencing on College desktop PCs is discouraged although is possible using personal devices and the College’s wifi system.

d) All staff and student conduct rules, GDPR-related issues such as the capture and broadcast of personal images/video/audio of others will apply to video conferencing in particular. So pay close attention and for example, only conduct webinar and video conferencing activity in enclosed meeting rooms rather than in clusters and classrooms.

A A A A

? AB A

It is expressly forbidden for users with administration permissions to use these to circumvent normal controls to install any software, or make changes to their desktop/laptop or other computing facilities for any personal or non-work related functions.

It is expressly forbidden for any member of staff to seek to be granted administrative permissions010m8411(d)-2.98462(m)-E18010m8411(d)-- Ts32dranteiv 11(d)--

A A A A Y

A

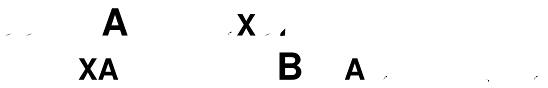
Computing facilities are provided for Suffolk New College’s business and curriculum purposes and responsible personal use is allowed provided there is no conflict with the interests or requirements of Suffolk New College. Suffolk New College does not accept liability for any personal loss or damage incurred through using the corporate computing facilities for private use.

A Y

In the light of changes in the business, technology, legislation or relevant standards it may be necessary to update this policy from time to time. Notification to all staff will be made when updates are available.

A YA A A

Suffolk New College wishes to promote the highest standards in relation to


A
X
XA
B
A

3. Deliberate introduction of viruses and malware to systems.

This list is not exhaustive, but sets the framework of Suffolk New College's approach to misuse of computing systems.

Suffolk New College has the right to monitor employees use of computer equipment where there is evidence to suggest misuse.