Suffolk
New
College

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

Equality Impact Assessment Tool

Name of Policy:
IT Acceptable Use Policy

		Yes/No	Comments
1	**Does the policy/guidance affect one group less or more favourably than another on the basis of:**		
	Race or ethnicity	No	
	Disability	No	
	Gender	No	
	Religion or belief	No	
	Sexual orientation	No	
	Age	No	
	Marriage and Civil Partnership	No	
	Maternity and Pregnancy	No	
	Gender Reassignment	No	
2	**Is there any evidence that some groups are affected differently?**	No	
3	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	N/A	
4	**Is the impact of the policy/guidance likely to be negative/**	No	
5	**If so, can the impact be avoided?**	N/A	
6	**What alternatives are there to achieving the policy/guidance without the impact?**	N/A	
7	**Can we reduce the impact by taking different action?**	N/A	

CONTENTS

1. INTRODUCTION

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.

1.1. RELATED POLICIES

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.

2. COMPUTING FACILITIES

2.1. DEFINITION

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.

2.2. AUTHORISATION, ACCESS AND DATABASE PRIVILEGES

2.3. DEFINITIONS

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.

2.4. CURRENT SCENARIO

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.

2.5. OWNERSHIP

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.

2.6. DESKTOP PCS (INCLUDING APPLE MACS)

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.

2.7. LAPTOP PCS (INCLUDING TABLET PCS, IPADS AND ANDROID TABLETS)

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.

2.8. MOBILE DEVICES

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 event that a device is stolen, staff will be expected to report the theft to the police, obtain an incident number and contact IT Services as soon as possible. IT Services, in conjunction with the Finance department, will ensure the mobile service is stopped.

Users of mobile devices must not change technical settings or interfacing configuration with laptops or other equipment without first consulting IT Services.

Records of billing for voice or internet access that is made using Suffolk New College-owned mobile devices are checked.

Staff members shall be held responsible for any abnormal charges incurred on the device and it is strongly discouraged that devices are used for any personal communications or non-work related internet activity.

2.9. LOAN EQUIPMENT

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.

2.10. PERSONAL EQUIPMENT USED TO ACCESS COLLEGE DATA AND SERVICES

With the increase in Remote Working as well as BYOD the College is now exposed to higher risk in terms of College data being accessed on devices, computers, laptops and mobile phones which are not centrally managed by the College.

It is not possible for the College to offer support on personal devices due to inherent legal, privacy and liability reasons.

However, as a policy:

Staff are required to undertake some basic steps to help safeguard College data and services:

1) Staff are required to ensure that the computer or device they are using is set to automatically update software and apps as well as Windows/Apple updates. Updates must not be turned off.

2) Desktop and laptop/tablet computers running Windows, Apple or Linux are required to have some form of anti-virus and anti-malware protection installed and that this is also set to update itself at least weekly.

   All anti-virus and anti-malware software must be ‘turned on’ conducting scanning as data is accessed.

   Windows 10 computers for example include Windows Defender which should be enabled.

3) Personal firewalls included with desktop/laptop computers should also be enabled.

4) If available we strongly advise turning on internet filtering/malware website protection functions which are provided with broadband connections, often alongside parental filtering controls.

5) Any computer, laptop or mobile phone which is ‘old’ for example, older than 5 years is likely to be no longer receiving updates; so in particular

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.

2.11. Software and Apps

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.

2.12. Data Security

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.

Further information about backup of data can be found in the IT Services Backup and Restoration Policy.

2.13. Personal Data and the Data Protection Act

Suffolk New College maintains a notification to the ICO in compliance with the Data Protection Act 2018. This notification is held on a public register and contains details of the Agency's holding and processing of personal data.

The designated Data Protection Compliance Officer, the Vice Principal, must be informed of all collections of personal data through the annual audit. It is the responsibility of all Suffolk New College staff to ensure that personal data is held and processed within the terms of Suffolk New College's notification and in compliance with Data Protection principles.

Further information about Data Protection can be found on the Information Management pages of the staff intranet.

2.14. Personal non-work related Data

Users shall be aware that the College accepts no liability for the loss or damage or exposure of personal information and communications such as email that a user chooses to store on College systems – for example, emails to and from family members.

As part of the leaver process, HR will send letters to staff members reminding them to remove personal data from any College system and it is the responsibility of the staff member to conduct this activity.

It is thus strongly advised that no use is made of any Suffolk New College resource for any personal data or communications, however this is not expressly forbidden at this time.

2.15. Freedom of Information Act

Suffolk New College is subject to the provisions of the Freedom of Information Act (2000) which provides for the general right of access to information held by public authorities. Employees should be aware that the Act effectively extends rights available under the Data Protection Act to include all types of information held, whether personal or non-personal. Therefore, such data or correspondence may be provided to an applicant in the event of an access request.

2.16. Anti-Malware and Virus Protection

Anti-virus software is loaded on all computers as standard and is updated regularly via the network. Laptops that belong to the College must be returned to IT Services regularly or plugged into the network and switched on for updates to anti-virus software to be kept current.

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.

2.17. Password Security

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.

2.18. Network Access Security

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.

3. FURTHER GENERAL GUIDANCE

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 facilities, or hosted by third parties that will be used for any aspect of College activity, including learner communication, dissemination of information or other service that is linked to the Suffolk New College brand.

2. Publish content of any type on external websites containing information relating to Suffolk New College, including the use of social networking sites.

3. Enter into agreements on behalf of themselves or Suffolk New College via a network or electronic system.

4. Transmit unsolicited commercial or advertising material to other users of a network or to other organisations.

5. Utilise any College equipment or branding/identity for external business interests or personal gain.

4. ELECTRONIC MAIL

4.1. USE AND RESPONSIBILITY

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.

4.2. CONTENT

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.

4.3. Privacy

E-mail messages to or from you cannot be considered to be private or confidential. Although it is not policy to routinely examine the content of individual e-mail, Suffolk New College reserves the right to monitor messages, at any time, for specific instances in which there is good cause for such monitoring or some legal obligation to do so.

Good cause shall include the need to fulfil legislative obligations, detect employee wrongdoing, protect the rights or property of the organisation, protect IT system security or to comply with legal process.

Messages sent or received may be copied and disclosed by Suffolk New College for lawful purposes without prior notice.

It is not permissible to access or to send e-mail from another employee’s personal account either directly or indirectly, unless you obtain that person’s prior approval for example by allocation of delegate permissions in Outlook.

4.4. Phishing and Scam / Fake Emails

A major risk which has increased in recent times are fake or scam emails which are sent with the intent to fool the recipient into opening, clicking on links, installing software, opening attachments or carrying out actions which in some way grant access to the sender to data/funds or other information.

The College’s Cyber Security Policy includes measures to safeguard against such attacks, however the role of the staff member still remains at the main protection against this form of threat.

Staff are required to:

a) Undertake awareness training and use links provided on the staff intranet to inform and educate themselves on phishing techniques and how to spot them.

b) Refrain from forwarding suspect emails or opening them or responding in any way and seeking advice if unsure from IT Services.

c) Report any instance where through error or suspicion, they believe that they may have responded to a scam/fake or suspicious message to IT Services as soon as possible.

4.5. MESSAGE FILTERING

For further information please see the IT Services Email and Transmission and Monitoring Policy.

5. INTERNET USAGE

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, religion/culture, national or regional origin, sexual orientation/identity, or disability under the sovereign law of the country in which the web server hosting the published material is sited.

Strictly, material must not be accessed from the web which would be objectionable on the above grounds under the sovereign law of the countries in which the networks transporting the material are sited or which would violate the Acceptable Use Policies of those networks.

Given the impracticality of assessing the exact legal position with regard to the previous two paragraphs, Suffolk New College Acceptable Use Policy governing material that could be objectionable on the above grounds is grounded in English law, on which basis it is reasonable to expect Suffolk New College employees to have good awareness and to be able to exercise good judgement. If in doubt over a specific case, please escalate through your line manager.

Once information is published on the worldwide web anyone from anywhere in the world can access it. It is therefore critical that material of a sensitive nature should not be published on public web sites, including social media platforms.

All Internet usage from the Suffolk New College network is monitored by automated methods and logged. Reporting on aggregate usage can performed when required for the purposes of audit.

When specific circumstances of abuse warrant it, individual user web access log will be investigated and linked to the relevant employee’s user account. Such an investigation may result in action via Suffolk New College’s Disciplinary Procedure and possibly criminal investigation.

Copyrights and licensing conditions must be observed when downloading software and fixes from the web sites of authorised software suppliers. Files so protected must never be transmitted or redistributed to third parties without the express permission of the copyright owner.

For further information regarding the categories of sites that violate acceptable usage please refer to the IT Services Internet Content Filtering Policy.

5.1. SOCIAL NETWORKING SITES

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.

Always include a disclaimer with a posting if it could be interpreted as an official statement or policy of Suffolk New College. For example:

“The views expressed are my own and do not necessarily represent the views or policy of my employer.”

5.2. SHARING OF CONTENT / DOCUMENTS USING GOOGLE WORKSPACE

The College currently enables the sharing of folders, documents and data stored on Google Workspace with external parties via the sending of links via email addresses.

It is strongly advised that this function is limited in use and care is taken to ensure that linked data can only be shared with the recipient of the email link.

This is because sharing a link at the ‘public level’ even with view-only permissions, will make that data/folder accessible to anyone on the internet who is forwarded that link.

It is therefore possible for breaches of information/security to occur unintentionally.

This is similar in risk to emailing, however, the Google Workspace/Drive platform adds further risks by enabling third parties to potentially edit/change data and access entire folder structures of data if a link to a folder structure is sent.

5.3. INSTANT MESSAGING, AND PERSONAL VOICE/VIDEO COMMUNICATIONS

There is now widespread use of web conferencing, Microsoft Teams, Google Meet and other voice/video/chat communication services throughout the College.

The same policies apply to these communications methods as apply to existing email and social media platforms.

This is an evolving area and at this time we advise the following guidance is followed:

a) Do not use personal Skype account or Gmail or other personal accounts for College web-conferencing – use Microsoft Teams or Google Meet using your College email address or @gapps.suffolk.ac.uk account only.

b) Most of the web-conferencing / webinar systems rely on software being installed on desktop PCs. College computers are equipped with Microsoft Teams and Google Meet support. Other products will require prior notification to IT Services, well ahead of any meeting, to install 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.

6. Use of Administrator level accounts for E-Mail, Internet and other non-necessary activities

This policy applies specifically to those members of staff such as IT Services or other areas such as Funding and Performance who have been granted ‘Administrator’ permissions access over EBS/Reporting and Integration Systems.

It may also apply to non-IT members of staff in other departments who may have been granted access to applications or third-party hosted systems.

Such members of staff shall ONLY use their Administrator permissions for the following purposes:

a) Actions that are required for their role and which can only be accomplished using the administrator permissions – such as installing software, making configuration/settings changes, assigning permissions/licences and rights to other members of staff.

b) Secondary actions such as conducting troubleshooting, carrying out system upgrades and updates and service checks.

6.1. Internet and Email Access with Administrator Permissions

a) There shall be no allowances or reasons for administrator level accounts to be used for normal email communications or phone/video conferencing situations.

   Instead, email and other forms of communication shall be limited to the extreme, for example, to download licence keys, or to login and obtain software updates/download links which require specific account login credentials.

b) Internet access shall also be limited as much as possible and used ONLY for the purposes of software/update download, registration of licences and other actions where normal operation of the system would not be possible without internet access.

   This includes the majority of cloud-based systems where browser access is required as a matter of course.

All staff granted any level of Domain/Local Administrator level access shall refrain from habitual or prolonged use of administrator level access for internet surfing, or video conferencing, or email access to minimise the threat of malware and other cyber threats using their enhanced permissions.

They are forbidden from logging into their normal desktop PCs as Admin accounts for prolonged periods of time or as a matter of habit and are required to use normal, non-administrator accounts.

6.2. Abuse or Attempts to Circumvent Controls

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 permissions by using any third party software or method not sanctioned in writing by the Director of IT Services.

In both cases, disciplinary action may result.

7. PRIVATE USE, LEGISLATION AND DISCIPLINARY PROCEDURES

7.1. PRIVATE USE

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.

8. UPDATES TO THIS POLICY

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.

9. RELEVANT LEGISLATION

This policy will comply with all Law and applicable regulations. This may include, but is not limited to the following:

1. The Investigatory Powers Act 2016
2. Computers' Misuse Act 1990
3. Protection from Harassment Act 1997
4. Sex Discrimination Act 1975
5. Race Relations Act 1976
6. Disability Discrimination Act 1995
7. Obscene Publications Act 1959
8. Telecommunications Act 1984
9. Protection of Children Act 1978
10. Criminal Justice Act 1988
11. Data Protection Act 2018
12. The Patents Act 1977
13. Copyright, Designs and Patents Act 1988
14. Defamation Act 1996
15. Freedom of Information Act 2000
16. Human Rights Act 1998

10. DISCIPLINARY AND RELATED ACTION

Suffolk New College wishes to promote the highest standards in relation to good practice and security in the use of information technology. Consequently, it expects and supports the integrity of its employees.

In exceptional circumstances, where there are reasonable grounds to suspect that an employee has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.

11. APPENDIX 1: EXAMPLES OF BEHAVIOURS WHICH REQUIRE THE USE OF THE SUFFOLK NEW COLLEGE DISCIPLINARY POLICY

11.1. GROSS MISCONDUCT

Examples:

1. Criminal Acts – for example in relation to child pornography.

2. Harassment – inappropriate e-mails or printed e-mails sent to a colleague, even if sent as a joke. Harassment can take a number of forms and is defined as unwanted conduct that affects the dignity of people within the workplace.

3. Obscene racist jokes or remarks which have been shared internally and externally – reflects on the image of employer and brings the organisation into disrepute.

4. Downloading and installation of unlicensed products.

5. Viewing sexually explicit materials, except where this forms an authorised part of the employee's job.

6. Visiting pornographic sites (adult top shelf materials). No reason such as 'testing filtering' exists to access such material; to test filtering software is working correctly, the IT Services team attempts to use a gambling website.

7. Chat rooms – sexual discourse, arrangements for sexual activity.

8. Violation of copyright that exceed allowanced made for curriculum/learning purposes, software media counterfeiting or illegitimate distribution of copied software

11.2. MISCONDUCT

Examples:

1. Frivolous use of computing facilities that risk bringing Suffolk New College into disrepute. The distribution of animated Greeting Card programmes or 'chain e-mails' beyond the internal e-mail system would represent examples of such misconduct.

2. Entering into contracts via the Internet that misrepresents Suffolk New College. Contracts are legally binding agreements and an employee must not enter into any agreements via the Internet to procure goods or services where Suffolk New College is liable for this contract, without first consulting Suffolk New College's procurement procedures.

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.