IT ACCEPTABLE USE POLICY AND AGREEMENT
LEARNERS

Version	Approved by Southend Borough Council Finance, Curriculum and Quality Group	Reviewed
001	September 2021	Every two years
Revisions:		

Introduction

The College provides a range of ICT resources which are available to learners. In order to ensure the safety of our systems, data and ultimately our learners, it is important that all users follow the guidelines detailed below.

This policy aims to:

- Promote the professional, ethical, lawful and productive use of the College's ICT systems and infrastructure.
- Define and identify unacceptable use of the college's ICT systems and any third-party systems.
- Educate users about their data security responsibilities.
- Describe why monitoring of the ICT systems may take place.
- Define and identify unacceptable use of social networking sites and college devices.
- Specify the consequences of non-compliance.

All users of the College's ICT systems, including College WiFi are invited to read and understand this policy. To confirm acceptance of the policy, users will be required to sign a consent form annually. Breach of this policy may result in disciplinary action. Support to be provided for learners as required.

The use by learners and monitoring by the College of its electronic communications systems may involve the processing of personal data and is therefore regulated by the Data Protection Act 2018. Learners are referred to the College's Data Protection Policy for further information.

If you are in doubt and require clarification on any part of this document, please speak to your tutor.

Provision of ICT Systems

All equipment that constitutes the College's ICT systems is the sole property of the College.

Users must not try to install any software on the ICT systems without permission from the Network Manager. If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.

Individual laptop/desktop computers or ICT equipment may be removed at any time, without prior warning, for regular maintenance, reallocation or any other operational reason. Maintenance includes, but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.

Users are not permitted to make any physical alteration, either internally or externally, to the College's computer and network hardware.

Network access and security

All users of the ICT systems at the College must first be registered. Following registration, and where appropriate, a network user account will be created, consisting of a username, password and an e-mail address. All passwords should be complex to ensure data and network security. All user account details are for the exclusive use of the individual to whom they are allocated. Learners are responsible for ensuring their password remains confidential and their account secure.

All users are personally responsible and accountable for all activities carried out under their user account. Users must take all reasonable precautions to protect their user account details and must not share them to any other person, except to designated members of the Network Support Team for the purposes of system support. Users must report any security breach or suspected breach of their network, email or application account credentials to the Network Support Team as soon as possible.

Users should only access areas of the college's computer systems to which they have authorised access.

When any computer is left unattended, it must either be logged off or locked. Activity that threatens the integrity of the college ICT systems, or activity which attacks or corrupts

other systems, is forbidden. Users' internet activity must not compromise the security of the data on the college ICT systems or cause difficulties for any other users.
Under no circumstances should a learner use a staff computer account, unless being directly supervised by the account owner.

College Email

Where email is provided, it is for academic and professional use only. The College's email system can be accessed from both the college computers, and via the internet from any computer. Wherever possible, all college related communication must be via the college email address.

The sending of emails is subject to the following rules:

- Must not include offensive or abusive language.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature (received or sent) are not permitted and could result in prosecution.
- Sending of attachments which contain copyright material to which the College does not have distribution rights is not permitted.
- Do not forward emails with email contacts included or 'reply to all' if not relevant to the communication to ensure email address data is kept secure.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Learners must immediately tell a designated member of staff if they receive offensive or abusive communication and this will be recorded under our Safeguard system and the appropriate actions taken if necessary under the College's Safeguarding Policy.
- College email addresses and other official contact details will not be used for setting up personal social media accounts.
- Where possible emails must not contain personal opinions about other individuals, e.g. other staff members or learners. Descriptions of individuals must be kept in a professional and factual manner.
- Learner email accounts are not able to contact anyone outside of the College's systems, they are for the sole purpose of communicating within the College.

Internet Access

Internet access is provided for academic and professional use.
The College's internet connection is filtered, therefore, inappropriate material is not accessible onsite. However, if inappropriate websites or links are accessed this must be reported immediately to Network Support network@southend-adult.ac.uk.

Learners must not access material which could be regarded as illegal, offensive, abusive or connected to violent crime, sexual abuse, drugs, substance misuse or linked to radicalisation.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, inappropriate use of the internet or e-mail systems (Including personal accounts) by viewing, accessing, transmitting or downloading any of the following material. (This list is not exhaustive):

- accessing and sharing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- transmitting a false and/or defamatory statement about any person or organisation;
- sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others;
- transmitting confidential information about the College and any of its staff, learners or associated third parties;
- transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the College);
- downloading or disseminating material in breach of copyright;
- engaging in online chat rooms, instant messaging, social networking sites and online gambling;
- forwarding electronic chain letters and other materials;
- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.
- Sending, receiving, downloading, displaying or disseminating any material that has a sexual content or perceived sexual content that could be used for the purposes of sexual harassment.

Any such action will be treated very seriously and may result in disciplinary action up to and including dismissal and exclusion from the college.

Where evidence of misuse is found the College may undertake a more detailed investigation in accordance with our Learner Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary such information may be handed to the police in connection with a criminal investigation.

Social Media

The key requirements for learners are as follows:

- Learners have a responsibility to protect the reputation of the college, its staff and other learners and to treat staff and other learners with respect whilst using social networking sites.
- No college information or information about other persons related to the college, communications, documents, videos and/or images should be posted on any personal social networking sites.
- Users must not knowingly cause annoyance, inconvenience or needless anxiety to others (cyber bullying) this includes all forms of harassment including the use of sexualized language via social networking sites.
- No opinions or details regarding members of staff or other learners, which could cause offence or risk of harm to the individuals concerned, are to be posted.
- No photos or videos, which show learners of the college who are not directly related to the person posting them, should be uploaded to any site.
- No comment, images or other material may be posted anywhere, by any method that may bring the college, its staff, its learners or the profession into disrepute.
- Staff are prohibited from accepting “friend requests” from a learners’ social network account. Any contact with Staff should be done via College email addresses or by calling the College directly.
- No sending, receiving, downloading, showing, sharing, displaying or disseminating any material that has a sexual content or perceived sexual content, or images, text or drawings that could be used for the purpose of sexual violence, abuse or harassment.

Digital Media (Images, Videos etc.)

The use of digital media, specifically, where these media files or streams show other staff and learners is prohibited unless all persons depicted have consented to the recording. The consent will be recorded prior to any dissemination of the material and the material must only be used for the purpose it was intended and that the persons agreed to. The material may not be altered or edited to misconstrue the persons original intensions. The media may not be changed to fit any other purpose without permission from those depicted. The taking and uploading of images for malicious purposes or that otherwise cause distress regardless of intent may be classed as a breach of the Colleges Safeguarding Policy and where appropriate will be investigated as such. For more details about Safeguarding investigations and outcomes please see the Colleges Safeguarding Policy.

File Storage

Learners have their own cloud storage area (OneDrive), as well as access to a shared network drive. Any college related work should be stored in one of these locations. Personal files are not permitted on the network areas. Learners are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files. These storage areas are provided for the purpose of supporting learning. Access to these areas will end when you leave the College, the College has no duty to the learner to retrieve their data once they have left the College. All data stored remains the property of the college and should not be deleted unless it is in line with the Data Destruction Policy.

Monitoring of the ICT Systems

The college will regularly audit the use of its ICT systems. This includes websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of the college's ICT system is, or may be taking place, or the system is, or may be being used for criminal purposes. Any inappropriate material found will be deleted. Monitoring software is installed to ensure that use of the network is regularly checked by the Network Support team to ensure there are no pastoral or behaviour concerns or issues of a safeguarding or prevent.
Other reasons for monitoring the ICT systems include the need to:

- ensure operational effectiveness of the services provided;
- maintain the systems;
- prevent a breach of the law, this policy, or any other college policy;
- investigate a suspected breach of the law or any other college policies.

Failure to Comply with the Policy

Any failure to comply with the policy may result in disciplinary action. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal.

Any unauthorised use of the college's ICT systems, cloud-based ICT systems, the internet, e-mail and/or social networking site accounts, which the Network Manager considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority.

The college reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.

Bring your own device

Learners are able to use their own devices at the college. The College reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of the College's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms. This policy is not designed to offer protection for the device itself. The safety of the user's own device is the responsibility of the user.

Mobile devices within the context of this policy includes any mobile phone, tablet, laptop, MP3/iPod or other device which is capable of connecting with the internet or mobile networks or taking image or sound recordings.

Acceptable Use

- When in College learners can connect their device to the internet via the College's Public wireless network.
- All internet access via the Public network is logged and, as set out in the Acceptable Use policy, learners are blocked from accessing certain websites whilst connected to the College network.
- The use of camera, microphone and/or video capabilities are prohibited whilst in College unless this has been approved by the Network Manager. If approved, any pictures, videos or sound recordings can only be used for College purposes and cannot be posted or uploaded to any website or system outside of the College network.
- You must not use your device to take pictures/video/recordings of other individuals without their advance written permission to do so.
- It is the learner's responsibility to make sure their device is free from viruses and other malicious applications and should ensure that any anti-virus protection they have installed is up to date.

Non-Acceptable Use

- As a point of note; any apps or software that are downloaded onto the user's device whilst using the College's own network is done at the users risk and not with the approval of the College.
- Devices may not be used at any time to:
    - Store or transmit illicit materials;
    - Store or transmit proprietary information belonging to the college;
    - Harass others;

  - Act in any way against the College's acceptable use policy and other safeguarding and data related policies.
- Technical support is not provided by the College on the user's own devices

Security

- In order to prevent unauthorised access, devices must be password/ pin/ fingerprint protected using the features of the device and a strong password is required to access the College network.
- When using personal data, it is the user's responsibility to ensure they keep data secure on their device. This includes preventing theft and loss of data (for example through password protection and cloud back up) keeping information confidential (for example by ensuring access to emails or sensitive information is password protected) and maintaining that information.
- The College does not accept responsibility for any loss or damage to the user's device when used on the College's premises. It is up to the user to ensure they have their own protection on their own device (such as insurance).
- If information is particularly sensitive then users should ensure that the data is either appropriately secured or deleted from the device (including from any local copies which may have been stored on the device).
- In the event of any loss or theft of personal data, this must be reported immediately as a data breach in accordance with the College's Data Breach policy.
- The College may require access to a device when investigating policy breaches (for example to investigate cyber bullying or a safeguarding incident).
- The College will not monitor the content of the user's own device but will monitor any traffic over the College system to prevent threats to the College's network.

Disclaimer

- The College reserves the right to disconnect devices or disable services without notification.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the College's policy as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The College reserves the right to take appropriate disciplinary action up to and including summary dismissal for non-compliance with this policy.

IT ACCEPTABLE USE AGREEMENT

To be completed by all learners.

As a college user of the network resources/ equipment I hereby confirm that I have read and understood the IT Acceptable Use Policy and that I agree to follow the college rules (set out within this policy) on its use. I will use the network/ equipment in a responsible way and observe all the restrictions explained in the college acceptable use policy. If I am in any doubt I will consult the Network Manager.

I agree to report any misuse of the network to the Network Manager. Moreover, I agree to report any websites that are available on the college internet that contain inappropriate material to the Network Manager. I finally agree to ensure that portable equipment such as cameras, iPads or laptops will be kept secured when not in use and to report any lapses in physical security to the Network Manager.

Specifically, when using college devices: -

- I must not use these devices for inappropriate purposes
- I must only access those services I have been given permission to use
- I will not download, use or upload any material which is unsuitable within a College setting or that may cause disruption to the College network.

If I do not comply with the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that learners under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

I understand that the College will monitor communications in order to uphold this policy and to maintain the College's network (as set out within this policy).

Consent is built into the consent protocol and form submitted annually.

Data Protection Officer: Judicium Consulting Limited Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com Web: www.judiciumeducation.co.uk Telephone: 0203 326 9174