IT ACCEPTABLE USE POLICY AND AGREEMENT

STAFF AND VOLUNTEERS

Version	Approved by Southend Borough Council Finance, Curriculum and Quality Group	Reviewed
002	**September 2021**	**September 2022**
Revisions: **The addition of Video Conferencing and Home Working in light of Covid (October 2020)** **Bring your own device section added (September 2021)**		

Introduction

This policy is designed to enable acceptable use for staff, governors and volunteers.

The College provides a range of ICT resources which are available to staff members, volunteers and governors. In order to ensure the safety of staff, governors and volunteers and our ultimately learners, it is important that all staff members, governors and volunteers 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 external 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.

This policy applies to staff members, governors, volunteers. All users of the College's ICT systems are expected to read and understand this policy. To confirm acceptance of the policy, users will sign a IT Acceptable Use Agreement which is attached to this policy. Breach of this policy may result in disciplinary action.

The use by staff and monitoring by the College of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff 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 the PA to the Principal.

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.

The Network Manager is responsible for purchasing and/or allocating ICT equipment to individuals. 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, 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. Staff are responsible for ensuring their password remains confidential and their account secure. Passwords must be changed regularly.

All users are personally responsible and accountable for all activities carried out under their user account(s). 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 be allowed to 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:

- Language must not include swear words, or be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.
- Sending of attachments which contain copyright material to which the College does not have distribution rights is not permitted.
- When sending an email to a number of recipients (over 5) use the 'BCC' – blind copy – option to ensure the list of emails remains GDPR secure.
- Don't 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 use of personal email addresses by staff for any official college business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email or password protection.
- Emails should never contain learner's full names either in the subject line or in the main body of the text. Initials should be used wherever possible.
- Access to college/setting email systems will always take place in accordance with data protection legislation and in line with other appropriate college/setting policies e.g. confidentiality.

- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the relevant files/records: the 'Safeguard – the college's online reporting system.
- Staff will be encouraged to develop an appropriate work life balance when responding to email.
- Emails sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on college headed paper would be.
- 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, children or parents. Descriptions of individuals must be kept in a professional and factual manner.

Internet Access

Internet access is provided for academic and professional use.

The College's internet connection is filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasions it might be possible to view a website which is inappropriate for use in a college. In this case the website must be reported immediately to Network Support.

Staff must not therefore access from the College's system any web page or any files downloaded from the web which could be regarded as illegal, offensive, in bad taste or immoral.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

- Accessing 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, students 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.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found the College may undertake a more detailed investigation in accordance with our 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.

Digital cameras

The college encourages the use of digital cameras and video equipment; however staff should be aware of the following guidelines:

- Photos should only be named with the learner's name if they are to be accessible in college only or if specific approval has been given via the photo consent process
- All photos should be downloaded to the college network and deleted from devices as soon as possible.

File Storage

Staff members have their own personal area on the network, as well as access to shared network drives. Any college related work should be stored on one of these network drives. Personal files are not permitted on the network areas. Staff are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files. Any files stored on removable media must be stored in accordance with the information access and security policy, summarised as follows:

- If information/data has to be transferred it must be saved on an encrypted, password protected, storage device
- No college data is to be stored on a home computer, or un-encrypted storage device.

- No confidential, or college data which is subject to the Data Protection Act 2018 should be transferred off site unless it is sent by secure email.

Mobile Phones

Mobile phones are permitted in college, with the following restrictions:

- They are not to be used when members of staff are directly supervising or working with learners. Whilst members of staff are working in the learning spaces they should be securely stored in a bag/cupboard/locker.
- All phone contact with parents/carers regarding college business will be through the college's phones. Personal mobile numbers should not be given to parents/carers at the college.

Social networking

The College has a Social Media Policy which should be read in conjunction with this policy. The key requirements for staff are as follows:

- Staff members have a responsibility to protect the reputation of the college, staff and students at all times and that they treat colleagues, students and associates of the college with professionalism and respect whilst using social networking sites.
- Social networking sites should be used responsibly and users should ensure that neither their personal or professional reputation and/or the college's reputation, nor the reputation of individuals within the college are compromised by inappropriate postings.
- Use of social networking sites for college business is not permitted, unless via an officially recognised college site and with the permission of the Marketing Officer.
- Members of staff will notify the Marketing Officer if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the college/setting.
- No college information, communication, documents, videos and/or images should be posted on any personal social networking sites.
- No details or opinions relating to any learner are to be published on any website.
- Users must not knowingly cause annoyance, inconvenience or needless anxiety to others (cyber bullying) via social networking sites.
- No opinions regarding another member of staff, which could cause offence, 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 other than the college's Website.
- No comment, images or other material may be posted anywhere, by any method that may bring the college or, the profession into disrepute.

- Users must not give students access to their area on a social networking site, (for example adding a student as a friend on Facebook).
- Phones provided by the college to staff to be used in line with the same robust procedures

Video Conferencing

Staff may be required to use video conferencing to interact with staff, learners, parents/carers and governors remotely. Staff should ensure they follow good practice when using it including: -

- Only using video conferencing platforms recommended by the college.
- Using a college username.
- Ensuring the password to access the platform is complex.
- Not to share sensitive material over the platform.

Home Working

Staff may be required to work remotely and should ensure they follow good practice when doing so, including: -

- Ensuring sensitive data is secured away and not shared with family or friends.
- Only using college approved devices and not personal devices.
- To avoid sharing personal data of third parties with others.
- To secure away any work devices safely.

Monitoring of the ICT Systems

The college may exercise its right to monitor 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 nature.

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, this policy, or any other college policy.

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

Staff are able to use devices at work and outside of work for work related activities provided the terms of this policy are met. 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

- By accessing the College's systems and networks, it is likely that staff will use personal data and so must abide by the terms of the Data Protection Act 2018 when doing so (including ensuring adequate security of that personal information).
- When in College staff should connect their device via the College's wireless network for security.
- When out of College, staff should access work systems on their mobile device using the webmail and VPN options managed by Network Support.
- All internet access via the network is logged and, as set out in the Acceptable Use policy, employees 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.

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 staff, governors and volunteers

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 staff 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