Southern Regional College

BRING YOUR OWN DEVICE POLICY

Process Area	**ICT**
Reference Number	**ICT 003**
Directorate	**Finance and Planning**

Issue No	**Date**	**Details**	**Author**	**Approved**	**Next Review**
001	Feb 2018	First Issue	S Todd	Governing Body	Jan 2021
002	Jan 2021	2nd Issue with Updates	TMcG	Governing Body F&GP	Oct 2022
003	Oct 2022	Policy updated to include new policy template and references to technical controls added.	ST, LC	Governing Body	Feb 2023
004	Feb 2023	Policy updated to include details on the College Mobile Device Management Platform and its capabilities and updated Roles and Responsibilities.	ST, LC	Governing Body	May 2025
005	May 2025	Definitions and Compliant Device added	ST, JMG	Governing Body	May 2028

If requested, the College will make the policy available in alternative formats to accommodate visual impairments. The policy can also be downloaded from the College website and made available in alternative languages upon request.

1 POLICY STATEMENT

1.1 Executive Summary

This policy defines acceptable use by SRC users whilst using *their own* devices for accessing, viewing, modifying, and deleting of SRC held data and accessing its systems and networks.

1.2 Intended Audience

This policy document applies to:

- All Users (staff, students, governing body members and guests) accessing SRC services.

1.3 Assumptions and Constraints

The College is responsible for ensuring that Personal Data is properly safeguarded and processed in accordance with the United Kingdom General Data Protection Regulations (UK GDPR) [1] and the Data Protection Act 2018 (collectively referred to in this document as Data Protection Legislation).

Southern Regional College ("the College") - is a data controller, for the purposes of Data Protection Legislation. It is assumed that all staff have an awareness of Data Protection Legislation and that they understand the consequences of the loss of College owned personal data.

1.4 Governance

Access to and use of IT resources and networks, at the College, is regulated by the Network Acceptable Use Policy available at https://www.src.ac.uk

The policy will be subject to review, in line with the College policy review schedule.

1.5 Device Management

To use a personal device to access College Data, users must enrol their device on the College Mobile Device Management Platform. Once enrolled the College will have access to control College Data and the device. This includes the capability to remotely wipe the enrolled devices should there be a verifiable risk to College data.

2 SCOPE

This policy applies to all College users (employees, temporary staff, students, governing body members, consultants and third- party agents) and includes mobile devices personally owned that are used to access the College's data and information resources.

[1] As a result of the United Kingdom's decision to exit the European Union, from December 2020 the United Kingdom General Data Protection Regulation (UK GDPR) will replace the GDPR 2018.

3 DEFINITIONS

BYOD	Bring Your Own Device refers to Users using their own device (which is not owned or provided to them by the College) to access and store College information, whether at the place of work or remotely, typically connecting to the College's Wireless Service.
Data Controller	The Data Controller is a person, group, or organisation (in this case the College) who determines the purposes for which and the manner in which any personal data are not, or are to be, processed.
User	A member of staff, enrolled student, contractor, visitor, or another person authorised to access and use the College's systems.
EduROAM	EduROAM (educational roaming) is an international secure wireless roaming service for users in research, higher education, and further education. It provides researchers, lecturers and students easy and secure Internet access at the College or when visiting an institution other than their own.
Open Public Wi-Fi	Wi-Fi networks which are not password protected and therefore vulnerable to malicious activity.
College Systems	Refers to technology platforms provided by the college for both staff and student devices.
College Data	Data stored on college systems where access is limited to staff use only e.g. Data stored on College information systems.
Compliant Devices	Devices owned by staff members which are approved for access to college data and systems. Staff devices are only permitted access to College Data if using a Compliant Device.

4 ROLES AND RESPONSIBILITIES

4.1 Chief Executive

The Chief Executive is responsible for:

- Ensuring guidance and procedural notes are approved in accordance with College governance arrangements for issue to staff.

4.2 Director of Finance and Planning

The Director of Finance and Planning is responsible for:

- Providing clear direction and visible senior management support for all security initiatives.
- Promoting security through appropriate commitment and adequate resourcing, in conjunction with the SMT and relevant personnel; and
- Deputising, as required, for the Chief Executive in respect of ICT security responsibilities.
- Ensuring compliance with relevant Data Protection legislation and GDPR regulations.

4.3 Assistant Director for ILT Development and ILT Systems

The Assistant Director for ILT Development and ILT Systems is responsible for:

- Ensuring ICT network security risks are being managed effectively.
- Ensuring all staff and students are aware of their responsibilities for network security and any related guidance notes.

4.4 Head of ICT and Network Services

The Head of ICT and Network Services will be responsible for:

- Implementing systems to segregate BYOD users from the core College network users.
- Implement technical controls to manage access to core internet-based applications.
- Maintain list of applications authorised for access.
- Provide a secure remote access service to authorised College users.
- Provide advice and guidance on all aspects of this Policy.

4.5 User Responsibilities

When using a mobile device such as a laptop, smartphone, or tablet, whether personal or College owned, to connect to the College network and access College systems and data, you are personally responsible for keeping data secure and must:

- Ensure that you adhere, at all times, to the College Acceptable Use Policy.
- Only use devices that are approved for use to access College Data and Systems. For staff these must be compliant devices.
- Ensure you keep College information and data securely. This applies to information held on your own device, as well as on College systems.
- If prompted to do so users must enrol their device on the College Mobile Management Platform.
- Assist and support the College in carrying out its legal and operational obligations with regard to College data and information stored on your device.
- You are required to co-operate with officers of the College when they consider it necessary to access or inspect college data stored on your device.
- Use the EduROAM service provided by the College to access the internet when on College premises or in other locations where EduROAM is available including other Colleges and Universities.
- Familiarise yourself thoroughly with the mobile device and its security features so you are able to ensure the safety of College information.
- Ensure that separate accounts are used on devices shared with family members.
- Ensure that all relevant security (firewall) and anti-virus features are enabled, where appropriate.
- Maintain the device by ensuring both the operating system and additional software (Apps) are regularly patched and upgraded.
- Set appropriate passwords, passcodes, passkeys or biometric equivalents. These must be of sufficient length and complexity for the particular type of device and will be enforced where possible by the College IT Systems.
- Install and configure tracking and/or wiping services, where the device has this feature.
- Take responsibility for any information that is downloaded onto the device.
- Take reasonable steps to prevent loss to their mobile device.
- Maintain the integrity of data and information accessed on the device

- Seek advice and guidance if you are in doubt about what information you should be storing on your device and how to handle it.
- Keep information stored on a personally owned device to the absolute minimum that is required to perform your role.
- Ensure that confidential information is not retained on the device for longer than is necessary.
- Avoid open public wi-fi connections as these pose information security risks and should be avoided especially when accessing sensitive College information.
- Report all information security incidents arising from mobile or remote working to IT Services.
- You must also cooperate with College officers in wiping the device remotely, even if such a wipe results in the loss of your own data, such as photos, contacts and music.
- Ensure that when a personally owned device is disposed of, sold or transferred to a third party all College information is securely and completely deleted.
- **MUST NOT** attempt to circumvent the device manufacturer's security mechanisms in any way, for example 'jailbreak' the device.

5 PROCEDURE FOR IMPLEMENTATION

5.1 Introduction

If you wish to BYOD to access College systems, data, and information you may do so, provided that you follow the provisions of this policy and the advice and guidance provided through the IT Services Help Desk.

Access is granted on 2 levels:

1. Access to college guest Wi-Fi networks for internet access e.g. EduROAM - (Available to all users).
2. Staff Access to College Data - (Limited to Compliant Devices).

The College reserves the right to refuse, prevent or withdraw access to Users and/or particular devices or software where it considers that there is unacceptable security, or other risks, to its staff, students, business, reputation, systems or infrastructure.

Compliant devices are limited to those running supported versions of mobile operating systems for IOS and Android. It should be noted that Windows and Mac OS will no longer be Compliant devices for staff BYOD.

Technical policies shall be implemented to ensure that certain conditions are met before access to College platforms is provided. These include setting:

- Minimum operating system requirements
- Password compliance
- Firewall requirements
- Antivirus requirements
- Preventing access from unsupported devices

By accessing EduROAM for BYOD the following internet-based services will be made available:

- Internet access in line with College filtering rules.
- VLE Services.

- Office 365 including email accounts, SharePoint, TEAMs, and OneDrive access.
- Licensed software Applications which are available remotely subject to licensing.

Certain services hosted on the internal college network will not be available, including:

- Home drives (H drives).
- College printing facilities.
- Specialist software where licensing restrictions apply.

Access to services hosted on the College private network will be made available to users via remote access services. This facility is only available to staff users and authorised remote access users.

5.2 Advice and Guidance

Advice and guidance on all aspects of this Policy are available via the IT Services Help Desk and Frequently asked questions on SharePoint and VLE platforms.

Advice and guidance on Data Protection Legislation is available from the College's Data Protection Officer.

EduROAM is a free to use wireless service offered with Southern Regional College and many other further education and higher education institutions.

Where EduROAM is available, staff and students can connect to it using their college e-mail address and password.

- Staff – username@src.ac.uk
- Students – studentid@students.src.ac.uk

This service is not available to students from the Schools Partnership Program.

5.3 System, Device, and Information Security

Staff can be provided laptops in order to access to core services via remote access, subject to approval from their Head of Department/Faculty.

Staff wishing to use their own device may do so using a compliant device, however the College will place restrictions on the services and apps that they may use to access College information. When using compliant devices, the storing of College information on personal devices should be kept to within College approved apps. The College acknowledges that data may make its way on to devices via email attachments for example, in these circumstances downloading the attachments to apps not approved by the college is prohibited.

Further advice on securing personal devices (including advice on the risks of downloading untrusted Apps) is available from the IT Service Help Desk.

5.4 Monitoring of User Owned Devices

The College will not monitor the content of your personal devices; however, the College reserves the right to monitor and log data traffic transferred between your device and College systems, both over internal networks and entering the College via the Internet.

To ensure the integrity of college systems staff will be required to present evidence that their personal device meets requirements for compliance with security accreditation. In some instances, staff will be required to bring their device to IT services. Any request for evidence or bringing their device into IT Services must be completed within 2 weeks.

In exceptional circumstances, for instance where the only copy of a College document resides on a personal device, or where the College requires access in order to comply with its legal obligations (e.g., under Data Protection Legislation, the Freedom of Information Act 2000, or where obliged to do so by a Court of law or other law enforcement authority) the College will require access to College data and information stored on your personal device.

Under these circumstances all reasonable efforts will be made to ensure that the College does not access your private information. Under some circumstances, for example where you legitimately need to access or store certain types of information, such as student or financial records on your own device, you must seek authority from your Line Manager. The College may then need to monitor the device at a level which may impact your privacy by logging all activity on the machine. This is in order to ensure the privacy, integrity and confidentiality of that data. You are required to conduct work-related, online activities in line with the College's Acceptable Use Policy. This requirement applies equally to BYOD.

5.5 Support

Where possible the College supports as broad a range of devices as possible, but you have a responsibility to learn how to use and manage your device effectively in the context of this policy. Help and advice is available on a reasonable endeavours basis, via the IT Service Help Desk.

The College takes no responsibility for supporting, maintaining, repairing, insuring or otherwise funding employee-owned devices, or for any loss or damage resulting from support and advice provided.

5.6 Use of Personal Cloud Services

Personal data as defined by Data Protection Legislation and College confidential information may not be stored on personal cloud services.

5.7 Breach of the Guidelines

If any user is found to have acted in breach of these guidelines, they will be dealt with in accordance with the College's Disciplinary Procedure. This may lead to termination of employment for employees, termination of a contract in the case of temporary staff, consultants or third-party agents and expulsion in the case of a student

5.8 Equality and Diversity

This Policy has been reviewed for accessibility and inclusion purposes and has positive benefits, allowing the use of a broad range of devices to meet individual needs.

5.9 Feedback

The College welcomes feedback on this Policy.

6 DISTRIBUTION

- All Staff and Learners
- Website

7 RELATED DOCUMENTS

- Network Acceptable Use Policy.
- ICT Network Security Policy.
- Mobile and Remote Working Policy.
- Information Handling Policy.

8 FLOWCHART

None.