BRING YOUR OWN DEVICE POLICY

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

Issue No	Date	Details	Author	Approved
001	Feb 2018	First Issue	S Todd	Governing Body
002	Jan 2021	2nd Issue with Updates	TMcG	Governing Body

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 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 Southern Regional College, is regulated by the Network Acceptable Use Policy available at http://www.src.ac.uk

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

2 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.

[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 PROCEDURE FOR IMPLEMENTATION

3.1 Introduction

This policy covers the use of non-College owned electronic devices to access corporate systems and store College information, alongside their own data. Such devices include, but are not limited to, smart phones, tablets, laptops and similar technologies. This is commonly known as 'Bring Your Own Device' or BYOD. This policy is complimentary to the SRC Network Acceptable Use policy.

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.

It is the College's intention to place as few technical and policy restrictions as possible on BYOD subject to the College meeting its legal and duty of care obligations.

The College, as the Data Controller, remains in control of the data regardless of the ownership of the device. As a User you are required to keep College information and data securely. This applies to information held on your own device, as well as on College systems.

Staff of the College are required to 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.

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.

Staff and Students may 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.

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

- Internet access in line with College filtering rules.
- Moodle and VLE Services.
- Office 365 including email accounts, TEAMs and OneDrive access.
- Licensed software Applications which are made 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 staff via remote access services. This facility is only available to staff users.

3.2 Advice and Guidance

Advice and guidance on all aspects of this Policy are available via the IT Services Help Desk:

Email: ITservices@src.ac.uk

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.

3.3 System, Device and Information Security

The College takes Information and Systems Security very seriously and invests significant resources to protect data and information in its care.

The use of your own device **MUST** adhere to the College's Network Acceptable Use Policy.

In particular, when you use your own device as a work tool, you MUST maintain the security of the College's information you handle (which includes but is not limited to viewing, accessing, storing or otherwise processing).

Staff wishing to use their own device may do so, however the College will place restrictions on the services and apps that they may use to access College information. The College will, were possible, provide access to core services via remote access. Therefore, 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.

All devices used for storing or processing College data and content must have industry standard security passwords in place and that this security mechanism is used to protect that device. Shared devices must have individual accounts with passwords. Single user devices e.g., Mobile Phones and Tablets should only be used if exclusively used by the member of staff and where a password/PIN exists.

Where a staff member uses their own device to access and store data that relates to the College then it is their responsibility to familiarise themselves with the device sufficiently in order to keep the data secure. In practice this means:

- Preventing theft and loss of data (using PIN/Password/Passphrase lock)
- Keeping information confidential, where appropriate.
- Maintaining the integrity of data and information.

If you are in any doubt as to whether particular data can be stored on your device, you are required to err on the side of caution and consult with your manager or seek advice from the IT Services Help Desk. Where information is stored on your device it should be kept to the absolute minimum that is required to perform your role.

You MUST:

- Use the device security features, such as a PIN, Password / Passphrase and automatic lock to help protect the device when not in use.
- Ensure that on shared devices, a separate user account and password is created to prevent other unauthorised device users accessing College systems.
- On personal devices, users must ensure that the device is not accessed by other users who could potentially access College systems.
- Keep the device software up to date, for example using Windows / Apple Update or Software Update services.
- Activate and use encryption services and anti-virus protection (ensure kept updated if your device features such services.
- Install and configure tracking and/or wiping services, such as Apple's 'Find My iPhone app', Androids 'Where's My Droid' or Windows 'Find My Phone', where the device has this feature.
- Remove any College information stored on your device once you have finished with it including deleting copies of attachments to emails, such as documents, spreadsheets and data sets, as soon as you have finished using them.
- Limit the number of emails and other information that you are syncing to your device to the minimum required.
- Remove all College information from your device and return it to the manufacturers' settings before you sell, exchange or dispose of your device.

In the event that your device is lost or stolen, or its security is compromised, **you MUST** promptly report this to the IT Services Help Desk, in order that they can assist you to change the password to all College services (it is also recommended that you do this for any other services that have accessed via that device, e.g., social networking sites, online banks, online shops). 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.

You MUST NOT attempt to circumvent the device manufacturer's security mechanisms in any way, for example 'jailbreak' the device.

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

3.4 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.

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.

3.5 Support

Where possible the College supports all devices, 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.

3.6 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.

3.7 Compliance Sanctions and Disciplinary Matters

Compliance with this policy forms part of the employee's contract of employment and failure to comply may constitute grounds for action, under the relevant College staff/ student disciplinary policy.

3.8 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.

3.9 Feedback

The College welcomes feedback on this Policy.

4 DISTRIBUTION

- All Staff and Learners
- Website

5 RELATED DOCUMENTS

SRC Network Acceptable Use Policy – Regulations accepted by Users when granted access to the College Computer Network.

SRC ICT Network Security Policy – Regulates the manner in which Information Systems are managed to ensure the security of information assets.

SRC Mobile and Remote Working Policy – Regulates remote Access to College ICT Services.

6 FLOWCHART

None.