BRING YOUR OWN DEVICE (BYOD) POLICY

DATE CREATED	September 2023	**DATE OF NEXT REVIEW**	May 2025
POLICY OWNER(S)	Head of IT		
DESIGNATION	Centre		

Purpose of policy	Provide a policy for the centre on bringing your own device into the centre
Intended audience	All staff
Links to other policies	Data protection policy, information security policy, Communications, Email and Internet Policy, Internet Filtering Policy and other policies and privacy notices relating to the internet

1. Introduction

1.1. The St Elizabeth's Centre (Centre) is committed to the highest standards of information security and treats confidentiality and data security extremely seriously.

1.2. This bring your own device (BYOD) policy supplements the Centre's other policies and procedures, which together place obligations on staff to take appropriate measures to safeguard Centre information against unauthorised or unlawful use, accidental loss, destruction or damage, by extending and/or clarifying these obligations in relation to staff use of their own personal devices at work.

1.3. The purpose of this policy is to protect the Centre's confidential, commercially sensitive and personal information and to ensure the Centre can comply with our legal and regulatory obligations, including those regarding data protection, record retention and audit by setting out the circumstances in which the Centre may monitor your use of its systems; access, retrieve, remove and destroy data on your device; and the action the Centre may take if you fail to comply with the obligations contained within this policy.

1.4. Except where indicated, this policy does not form part of any employee's contract of employment and the Centre expressly reserves the right to amend it at any time. Changes made to this policy will be notified to staff on the Centre's Intranet.

2. Definitions

For the purposes of this policy:

business information	means business-related information other than personal information regarding service users, suppliers and other business contacts of the Centre;
confidential information	means trade secrets or other confidential information (either

	belonging to the Centre or to third parties) that is processed by the Centre;
personal information	(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;
your device	means all electronic devices, including laptops, tablets, personal digital assistants and other hand-held or portable devices, smartphones, and any other applications or technology that are used by you to access, store, create, copy or transmit Centre information and that are not owned or supplied by us or on our behalf.

3. Scope and Data Protection

3.1. The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the Centre, in whatever media. This includes information held on computer systems, hand-held devices, phones, paper records, and information transmitted orally.

3.2. This policy applies to all staff, including employees, temporary and agency workers, other contractors, interns, volunteers and apprentices.

3.3. All staff must be familiar with this policy and comply with its terms.

3.4. The Centre information covered by this policy may include:
- 3.4.1. personal information relating to staff, service users, suppliers;
- 3.4.2. other business information; and
- 3.4.3. confidential information.

3.5. This policy supplements the Centre's data protection policy, information security policy, Communications, Email and Internet Policy, Internet Filtering Policy and other policies and privacy notices relating to the internet, email and communications, document retention and the contents of those policies must be taken into account, as well as this policy.

3.6. All staff who adopt BYOD must comply with the Centre's data protection policy, information security policy and Communications, Email and Internet Policy and the data privacy standard detailed in paragraph 15 (Data privacy standard) of this policy.

3.7. This policy will entitle and enable the Centre access and process personal information on your device. The Centre relies on the following lawful bases for that processing:
- 3.7.1. it is necessary for the Centre to comply with its legal obligations to protect the personal information of its staff and third parties; and

3.7.2. it is necessary for the purposes of the Centre's legitimate interests, namely to protect its Centre information and the security of its systems.

3.8. We will review and update this policy in accordance with our data protection and other obligations. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy when it is adopted.

4. Obligations Regarding Information Security

4.1. It is in the interests of the Centre and its staff for staff to be able to do their work flexibly and effectively, and the Centre recognises that this may extend to you using your device for work purposes. In permitting you to use your device for work purposes, the Centre requires you to exercise all necessary care, take certain precautions and be responsible when using your device to connect to the Centre's IT systems and/or to access Centre information.

4.2. In order to protect Centre information, you are required to comply with the obligations set out below at all times, both during or outside of office hours and whether or not you are at your normal place of work.

4.3. If you do not comply with this policy, the Centre may revoke its permission for you to use your device for work purposes and may take other appropriate action (see paragraph 20 (Failure to comply with this policy) below).

4.4. If you have any questions about this policy, please contact the Head of IT or Data Protection Officer at the Centre.

5. Centre Information

5.1. All Centre information should be considered to be commercially valuable and you must protect it from loss, theft, misuse, inappropriate access, modification or disclosure. You should exercise an even higher degree of caution when accessing or working with sensitive information, in respect of which the impact of loss or unauthorised access may be even more serious than would ordinarily be the case.

5.2. Your obligations concerning data security generally (including regarding technical security measures and organisational security measures) are detailed in the Centre Information Security Policy.

6. Approved Devices and Registering your Device

6.1. The Centre will only consider permitting you to use your device in accordance with this policy if it is listed as supported below in paragraph 6.2. This approved devices list will be maintained and updated from time to time.

6.2. The following devices are supported:
  6.2.1. smartphones;
  6.2.2. tablets;
  6.2.3. laptops; and
  6.2.4. desktop computers.

6.3. Before using your device at work to connect to the Centre's IT systems and/or to access Centre information in accordance with this policy, you must:
  6.3.1. register your device with the IT department; and
  6.3.2. present your device to the IT department for approval, provisioning and configuration; and
  6.3.3. implement such technical security measures as the IT department require.

6.4. You are not permitted to use any device other than a device which has been registered and approved by the IT department to connect to the Centre's IT systems and/or to access Centre information. The Centre reserves the right to refuse or remove approval for your device to connect to its IT systems and/or access Centre information where it is of the reasonable opinion that the device is or may be capable of being used in a way that may breach this policy.

7. Acceptable Use

7.1. The Centre defines acceptable business use as activities that directly or indirectly support the business of the Centre.

7.2. The Centre defines acceptable personal use during Centre time as reasonable and limited personal communication or recreation.

7.3. Staff are blocked from accessing certain websites that the Centre considers inappropriate while connected to the Centre's IT network.

7.4. The camera and/or video capabilities of your device are not required to be disabled while on-site.

7.5. Your device may not be used at any time to:
  7.5.1. engage in any activity that constitutes a breach of any of the Centre's policies (such as the Centre's Communications, Email and Internet Security Policy);
  7.5.2. store or transmit illicit materials;
  7.5.3. store or transmit proprietary information;
  7.5.4. harass, bully or unlawfully discriminate against others;
  7.5.5. defame or criticise the Centre or its affiliates, customers, clients, suppliers, vendors and other stakeholders;
  7.5.6. engage in outside business activities; or
  7.5.7. breach any other laws or ethical standards,

7.6. The Centre has a zero-tolerance policy towards texting or emailing using your device while operating a Centre or personal vehicle. You must comply with any applicable law concerning the use of such devices in vehicles. In the UK, only hands-free talking is permitted while driving.

8. Security

8.1. In order to prevent unauthorised access, your device must be password or PIN protected using the features of the device. A strong password is required to access the Centre's IT network.

8.2. Chosen passwords must comply with the Centre's password policy, as set out in the Information Security Policy.

8.3. The device must lock itself with a password or PIN if idle for five minutes.

8.4. After five failed login attempts, the device must lock.

8.5. You must comply with the attached security protocols, which form part of this policy, and take all other reasonable efforts to secure your device whether or not it is in use and whether or not it is being carried by you.

8.6. Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the Centre's IT network.

8.7. Smartphones and tablets that are not present on the approved devices list are not permitted to connect to the Centre's IT network and/or to access Centre information (see paragraph 6 (Approved devices and registering your device) above).

8.8. Smartphones and tablets belonging to staff that are for personal use only are allowed to connect to the Centre's IT network.

8.9. Staff access to Centre information is limited based on user profiles defined by the IT department and automatically enforced.

8.10. Data on your device may be remotely erased by the Centre if:

8.10.1. there is a data breach or potential data breach involving Centre information relevant to your device;

8.10.2. your device is lost or stolen;

8.10.3. your password is lost or stolen;

8.10.4. you are suspended from work or placed on garden leave in accordance with your contract of employment;

8.10.5. you cease working for the Centre and you have not complied with your relevant obligations under paragraph 19 (Staff departure) below;

8.10.6. the IT department detects a virus, malware or other destructive program or code relevant to your device; or

8.10.7. there is a login failure on your device after 5 incorrect password attempts.

9. Care Responsibilities

9.1. As a controller, the Centre is responsible for ensuring that all processing of personal information which is under its control remains compliant with the Data Protection Act 2018, as amended from time to time, which implements Regulation (EU) 2016/679, General Data Protection Regulation (GDPR), together (the Data Protection Legislation). In particular, the Centre must:

9.1.1. use technical or organisational measures to ensure personal information is kept secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage;

9.1.2. implement appropriate technical and organisational measures to demonstrate that it has considered and integrated data compliance measures into the Centre's data processing activities; and

9.1.3. be able to demonstrate that it has used or implemented such measures.

9.2. The Centre is however mindful of the personal usage of approved devices and the privacy of staff. Technical and organisational measures taken by the Centre in relation to this policy will remain proportionate to the risks involved. The Centre will use reasonable endeavours not to access, use, copy or delete personal information (which is not also Centre information) held on your device unless it is absolutely necessary for legitimate business purposes.

10. Accessing and Using Centre Information

10.1. You are permitted to connect to or access only the following Centre IT systems from your device:

10.1.1. the Centre email system;
10.1.2. calendars
10.1.3. contacts
10.1.4. Kura
10.1.5. Pleo
10.1.6. Nooa
10.1.7. Client Wi-Fi access – please refer to Communications, Email and Internet Security Policy and Internet Filtering Policy

10.2. You must only use Centre information:

10.2.1. if you are an employee: for acceptable business uses;
10.2.2. if you are a supplier, subcontractor or consultant: to provide services to us; or
10.2.3. if you are a service user: to receive services from us; and not for any other purpose.

10.3. You must only use Centre information:

10.3.1. in accordance with the security protocols; and

10.3.2. in accordance with the attached separation protocols, which form part of this policy.

10.4. Centre information remains our property at all times, no matter what format it is in, where it is stored or how it is accessed.

10.5. In using your device for work purposes, you agree to give us access to any Centre information on your device immediately on our reasonable request. In this context, 'accesses include us being permitted to access, make copies of, recover or delete files (including all copies of files) containing Centre information from your device.

11. Regulatory Reasons and Audit

11.1. From time to time the Centre may need to access and/or audit your device (and the information and applications on it), in order to pursue the following legitimate business purposes (together the regulatory reasons):

11.1.1. to verify your compliance with this and other Centre policies;

11.1.2. to ensure that the Centre complies with its obligations to its regulators, the courts and other relevant official bodies (regulators);

11.1.3. to demonstrate to regulators that the Centre has been complying with its legal and regulatory obligations; and

11.1.4. to cooperate with any investigations, proceedings or other requests for information by the regulators.

11.2. In using your device as envisaged by the provisions of this policy, you authorise the Centre (or its authorised agents or representatives, such as auditors or regulators) to access and/or audit your device for regulatory reasons, as the Centre reasonably require from time to time. You agree to co-operate with and facilitate any such access and/or audit.

11.3. The Centre appreciates that your device will contain both Centre information and your personal information.

11.4. If you comply with the separation protocols and the security protocols, any intrusiveness or inconvenience to you of the Centre accessing and/or auditing your device is likely to be minimised.

12. Restrictions on Centre Rights of Access

When taking (or considering taking) action to access your device or delete data on your device (remotely or otherwise) in accordance with this policy, the Centre will, where practicable:

12.1. weigh up whether such action is proportionate in light of the potential damage to the Centre, its customers or other affected persons as a result of the Centre information risk, regulatory reasons or other relevant reasons;

12.2. consider if the Centre information risk, regulatory reasons or other relevant reasons could reasonably and effectively be dealt with in some other way (but appreciating Centre information risks and regulatory reasons in particular often require quick, decisive and urgent action); and

12.3. take reasonable steps to minimise loss of your personal information on your device, but the Centre shall not be responsible for any such loss that may occur.

13. Services the Centre Provides

The Centre reserve the right to (temporarily or permanently) disconnect, disable, restrict use of or modify at any time any services that it provides and that you access via your device at any time, for any reason and without prior notice.

14. Your Responsibilities Concerning Your Device

14.1. You are at all times responsible for:

14.1.1. purchasing your device, paying all device and carrier service costs, bills and tariffs for your device, including but not limited to voice and data usage charges;

14.1.2. repairs to and maintenance of your device and the associated costs, including costs required to replace your device;

14.1.3. running backups of your own data on your device at least monthly; and

14.1.4. ensuring periodic system/security upgrades are installed without delay when notified of their availability.

14.2. You agree that you use your device at your own risk and that the Centre will not be responsible for any losses, damages or liability arising out of its use (to the extent permitted under applicable law).

14.3. The Centre recommends that you personally insure your device (e.g. as part of a household insurance policy).

15. Data Privacy Standard

15.1. You are referred to the Centre's data protection policy, which establish the Centre's data privacy standard. You are required to act in a manner consistent with that standard during your employment and also in the operation of your device under this policy. This section highlights your key obligations when handling personal information on your device. It is non-exhaustive and does not substitute the obligations to which you are subject under the Centre's other policies.

15.2. You must provide the data subject with all the information required by the Data Protection Legislation as soon as possible after collecting/receiving the data. You must also check that personal information collected by a third party was done so in accordance with the Data Protection Legislation.

15.3. You cannot use personal information for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the data subject of the new purposes and they have consented where necessary.

15.4. You may only process personal information when performing your job duties requires it. You cannot process personal information for any reason unrelated to your job duties.

15.5. You may only collect personal information that you require for your job duties: do not collect excessive data. Ensure any personal information collected is adequate and relevant for the intended purposes.

15.6. You must ensure that when personal information is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Centre's record retention policy.

15.7. You must ensure that the personal information you hold is accurate, complete, kept up to date and relevant to the purpose for which it was collected. You must check the accuracy of any personal information at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out of-date personal information.

15.8. You must not keep personal information in a form which permits the identification of the data subject for longer than needed for the legitimate business purpose or purposes for which it was originally collected.

15.9. You will take all reasonable steps to destroy or erase from your device all personal information that is no longer required in accordance with the Centre's record retention policy. This includes requiring third parties to delete such data where applicable.

15.10. You must act responsibly in the processing of personal information and use reasonable and appropriate measures to protect it from accidental loss or damage.

15.11. You must follow all procedures and technologies we put in place to maintain the security of all personal information from the point of collection to the point of destruction. You may only transfer personal information to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

15.12. You must maintain data security by protecting the confidentiality, integrity and availability of personal information.

15.13. You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the Data Protection Legislation and relevant standards to protect personal information.

15.14. You may only transfer personal information outside the EEA in certain circumstances and you should check whether the applicable conditions apply before doing so.

16. Risks You Accept

16.1. You acknowledge that there are specific risks associated with you using your device for work purposes in accordance with this policy. These risks include the threat of viruses, malware and other software and/or hardware failures or programming, operating system or other errors that may result in loss of data (yours and/or Centre information) or your device not working properly or at all.

16.2. However, in consideration of you being allowed to use your device for work purposes in accordance with this policy, as the user of your device, you agree to accept and assume full liability for these risks (except for any liability that we cannot by law exclude or limit).

17. Theft or Loss of Device

17.1. If your device is lost or stolen, you must inform the IT department by no later than the next working day.

17.2. The quicker you inform the Centre of this and cooperate by providing such information and assistance as the Centre request, the more effectively the Centre will able to assess and contain any potential data security breach risk and any other relevant risks. This will in turn impact the level of our response and the action the Centre needs to take.

18. Data Security Breach

18.1. If you become aware of a breach of security, or believe that your device may have been accessed by an unauthorised person or otherwise compromised, you must inform the IT department as soon as possible and in any event by no later than close of business on the relevant day.

18.2. The Centre has legal obligations under the Data Protection Legislation. The quicker you inform the Centre of this and cooperate by providing such information and assistance as the Centre requests, the more effectively the Centre will able to assess and contain any potential data security breach risk and any other relevant risks. This will in turn impact the level of our response and the action we need to take.

19. Staff Departure

19.1. On your exit from the Centre (regardless of the reason for your exit) and prior to commencing any period of garden leave:

19.1.1. your access to the Centre IT system, its applications and all Centre information will cease;

19.1.2. your device will be delivered up to the Centre and de-provisioned; and

19.1.3. all Centre information on your device will be wiped (permanently deleted).

19.2. You are reminded that your obligations to keep Centre information confidential continue even after you cease working for the Centre.

19.3. Upon ceasing working for the Centre, as well as complying with all HR exit procedures, if the Centre request, you will sign a written declaration confirming your device contains no Centre information and/or allow us to inspect your device to confirm your device contains no Centre information. You will provide all necessary co-operation and assistance to the IT department in relation to this process.

20. Failure to Comply with this Policy

20.1. Failure to comply with this policy may result in disciplinary action including, where appropriate, revocation of access to Centre IT systems, suspension, dismissal and criminal prosecution. Disciplinary action may be taken whether the breach (or suspected breach) is committed during or outside of office hours and whether or not use of the device takes place at your normal place of work. As well as any specific rights the Centre has in this policy that apply where you breach particular provisions of this policy, your breach of your obligations under this policy will constitute a breach of your contract with the Centre and the Centre may exercise its rights under that contract. You will be required to co-operate with any investigation into suspected breaches of this policy, which may require you to provide the Centre with full access to your device and any relevant passwords and login details.

20.2. If you have reasonable grounds to suspect that someone else is in breach of this policy, you must inform the Centre immediately.

21. Policy Review

The Centre shall review this policy not less than biennially and otherwise as required in order to ensure that it remains up-to-date and fit for purpose. All questions, concerns, and other feedback relating to this policy should be communicated to the IT Manager.

22. Implementation of Policy

This Policy shall be deemed effective as of 01 September 2023. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.