CONNECTED LEARNING
Acceptable Personal Use of Resources and Assets Policy

Document Detail	
Category:	Information Governance
Authorised By:	CL Board of Trustees
Status:	APPROVED
Date Approved:	21 October 2020
Next Review Date:	Every 2 years – October 2022

Acceptable Personal Use of Resources and Assets Policy

What must I do? How must I do it?

Why must I do it?

ALL: To ensure we use our IT and other facilities resources effectively, making sure that our reputation is maintained and to ensure that staff working time is used efficiently on delivering our business outcomes

1. ***MUST***: You must use our facilities **economically**; your personal use must not create extra costs for us
   By checking with your manager or where you have any uncertainty over what is appropriate

2. ***MUST NOT***: You must not use our facilities to undertake any unlawful, libellous, immoral or offensive **activities**, including accessing, downloading, storing, creating, copying or disseminating offensive material. This includes, but is not limited to, pornographic, sexual, violent or criminal content and racist, sexist or otherwise discriminatory material
   By complying with the points of this policy

3. ***MUST NOT***: Personal use must not interfere with your **productivity** and how you carry out your duties
   You must only make personal use of our IT facilities outside of time you are recording or is designated as your 'working hours'

4. ***MUST NOT***: Personal use must not reflect adversely on our **reputation**
   By complying with the points of this policy

5. ***MUST NOT***: You must not leave **personal-use websites** open during your working time, even if they are minimised on your screen and you are not actively viewing/ using them
   Closing websites when you are not actively using them

6. ***MUST NOT***: You must not use browsers or access/ attempt to access sites that are knowingly **unacceptable**, even if this is in your own time
   By taking care over the sites you are about to open, including reading search report information before opening

7. ***MUST NOT***: You must not **send or forward** chain, joke or spam emails
   By deleting such items if you receive them

8. ***MUST NOT***: You must not use the Trust's facilities for **commercial purposes** not approved by us or for personal financial gain
   By checking with your manager where you have any uncertainty over what is appropriate

9. ***MUST NOT***: You must not use your access rights or identity as an employee to **mislead** another person, for personal gain or in any other way which is inconsistent with your role
   By checking with your manager where you have any uncertainty over what is appropriate

10. ***MUST NOT***: You must not **disclose** (in writing, speech or electronically) information held by us unless you are authorised to do so, and the recipients are authorised to receive it
    If you are not sure if you are authorised to disclose information, speak with your manager in the first instance

11. ***MUST NOT***: When you print, photocopy, scan or fax official-sensitive information, you must not leave the information **unattended**.
    If you are faxing information outside your immediate office, always make sure that there is someone waiting at the other end to receive it. For other devices, if there is no secure release facility which requires you to be present, you must ensure you wait for the process to complete and remove any originals and copies from the equipment

12. ***MUST NOT***: You must not **connect** any equipment to our IT network that has not been approved
    Check that equipment has been tagged or marked as an accepted and managed device before insertion/ connection

13. ***MUST NOT***: You must not do anything that would **compromise** the security of the information held by us, such as downloading/ spreading any harmful virus/ program or disabling or changing standard security settings
    IT controls should prevent your ability to download anything harmful, but if in doubt, contact your manager in the first instance.

14. ***MUST NOT***: You must not make personal use of the information available to you that is not available to the **public**
    If you wish to utilise Trust data in a personal capacity, you must make a formal request for information to the Chief Executive Officer

What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the Clerk to the Board of Trustees (tinaweavers@connectedlearningmat.co.uk)

Document Control

Version:	1
Date approved:	[Date]
Approved by:	[Name of authorising officer or board]
Next review:	[Approval date + review period]

References

- Data Protection Act 2018
- Human Rights Act 1998

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.