Essex Partnership University
NHS Foundation Trust

ANTI-VIRUS POLICY

POLICY REFERENCE NUMBER	CP76
VERSION NUMBER	V1.0
KEY CHANGES FROM PREVIOUS VERSION	Not Applicable
AUTHOR	[redacted] – Cyber Security Manager
CONSULTATION GROUPS	ICT
IMPLEMENTATION DATE	June 2019
AMENDMENT DATE(S)	Not Applicable
LAST REVIEW DATE	Not Applicable
NEXT REVIEW DATE	June 2022
APPROVAL BY INFORMATION GOVERNANCE & SECURITY SUB-COMMITTEE	28th March 2019
RATIFICATION BY QUALITY COMMITTEE	13th June 2019
COPYRIGHT	

POLICY SUMMARY

The purpose of this Anti-Virus and Malware Policy is to provide guidance in line with HMG and private sector best practice for the implementation of an organisation wide Anti-Virus and Malware Policy. Ensuring that the applicable and relevant anti-virus and malware security controls are set in place in line with the Department for Health, the wider NHS, health and social care and HMG requirements.

The Trust monitors the implementation of and compliance with this policy in the following ways;

Continual monitoring by ICT Services

Services	Applicable	Comments
Trustwide	✓	
Essex MH&LD		
CHS		

The Director responsible for monitoring and reviewing this policy is Director of Information Technology and Telecommunication

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

ANTI-VIRUS POLICY

CONTENTS

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

ANTI VIRUS POLICY

Assurance Statement

This policy provides assurance to the following requirements laid out by NHS Digital to comply with the Cyber Essentials Plus requirements –

Anti-virus or malware protection software been installed on all computers that are connected to or capable of connecting to the Internet. Has anti-virus or malware protection software (including program/engine code and malware signature files) been kept up-to-date (either by configuring it to update automatically or through the use of centrally managed service). Anti-virus or malware protection software been configured to scan files automatically upon access (including when downloading and opening files, accessing files on removable storage media or a network folder) and scan web pages when accessed (via a web browser). Malware protection software been configured to perform regular periodic scans (e.g. daily).

1.0 GENERAL

1.1 EPUT systems will run effective anti-virus and anti-malware software.

1.2 EPUT anti-virus and anti-malware software will be configured to detect and remove known viruses and malware.

1.3 All EPUT systems will run one of the NHS approved and supported anti-virus and anti-malware software packages.

1.4 All servers, desktops and laptops will be configured to run only one of the approved products at any time.

1.5 Anti-virus and anti-malware software will be kept up to date.

1.6 Anti-virus and anti-malware definition files will be kept up to date.

1.7 Anti-virus and anti-malware software updates will be deployed across the network automatically following their receipt from the vendor.

1.8 Virus and malware signature updates will be deployed across the network automatically following their receipt from the vendor.

1.9 Anti-virus and anti-malware software will be configured for real time scanning and regular scheduled scans.

1.10 Tamper protection will be enabled to prevent end users or malware altering the anti-virus and anti-malware software's configuration or disabling the protection.

1.11 All ICT equipment and removable media will be scanned for viruses and malware before being introduced to the EPUT network, system or device.

1.12 ICT systems infected with a virus and malware that the anti-virus or anti-malware software has not been able to deal with will be quarantined from the NHS network until virus free.

1.13 Any instance of virus or malware infection or detection will be documented and raised as a security incident.

2.0 ADMINISTRATIVE

2.1 Changes that are required to the settings of any of anti-virus or anti-malware products will follow the formal EPUT change control process.

2.2 ICT will ensure that all anti-virus and anti-malware products are regularly and correctly updated from the vendor service.

2.3 ICT may periodically test anti-virus and anti-malware defences by deploying a safe and non-malicious test file.

2.4 A log will be kept of all scans undertaken, these logs should record as a minimum:

- Date.
- Time.
- Addresses of areas scanned.
- Malware found.
- Any action taken by the anti-virus and anti-malware software (e.g. quarantine or delete).

2.5 To prevent misuse and tampering by unauthorised staff, all administrative settings in the deployed anti-virus and anti-malware products will be secured by means of a password.

3.0 MONITORING OF IMPLEMENTATION AND COMPLIANCE

3.1 ICT will monitor the anti-virus systems on a daily basis (during the working week) to ensure all devices are fully compliant with this policy.

3.2 Any system found in violation of this policy will require immediate corrective action.

3.3 ICT will ensure that any device complies with this policy prior to being installed for use within the business.

4.0 REFERENCE OTHER DOCUMENTATION

4.1 The following documents should be read in conjunction with this Policy and its associated procedural guidelines:

- CP59 Data Protection and Confidentiality Policy

END