Essex Partnership University
NHS Foundation Trust

ICT Procedure for Monitoring Anti-Virus

PROCEDURE REFERENCE NUMBER	CPG76
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	

PROCEDURE SUMMARY

This document outlines the procedure that ICT will undertake to ensure devices are compliant with the Trust's Anti-Virus Policy.

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

Monthly Reporting

Services	Applicable	Comments
Trustwide		
Essex MH&LD		
CHS		
ICT	✓	

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

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

ICT Procedure for Monitoring Anti-Virus

CONTENTS

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

ICT Procedure for Monitoring Anti-Virus

Assurance Statement

In accordance with the Trust's Anti-Virus Policy, all EPUT systems shall run effective anti-virus and anti-malware software.

1.0 INTRODUCTION

1.1 ICT will monitor the Anti-Virus systems on a daily basis (during working hours) to ensure systems are protected and up to date.

1.2 ICT will monitor the Anti-Virus systems on a daily basis (during working hours) to ensure any detected viruses or malware are dealt with.

1.3 ICT will produce Monthly reports detailing all attempted infections.

1.4 ICT will ensure any disposed devices are removed from the AV console.

1.5 ICT will provide the Asset Management Lead a list of all devices that have not been seen for more than 30 days and cannot be located.

2.0 DAILY TASKS

2.1 Check any outstanding virus alerts and clean.

2.2 Check any outstanding Potentially Unwanted Applications (PUA's) and clean.

2.3 Check all scanning errors and resolve any issues identified.

2.4 Ensure all connected devices are compliant with the AV policies

2.5 Ensure all connected devices are up to date (any devices reporting as unknown will need to be examined and any issue identified, resolved)

3.0 MONTHLY TASKS

3.1 Generate report detailing previous month's virus infection attempts and send to the Cyber Administrator.

3.2 Obtain a report from the asset management lead detailing devices that have been disposed in the last month and delete any identified devices from the console.

3.3 Investigate any device that has not be seen by the console for more than 30 days. If located, ensure the device is updated and initiate a full scan. If unable to locate the device, report it to the asset management lead.

4.0 REFERENCE OTHER DOCUMENTATION

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

- Anti-Virus Policy

END