

Anti-Virus Service

Contents

Anti-Virus Service.....	1
Service Overview and Benefits	1
Service Description	1
Supported Network	2
Virus Detection Event.....	2
Unsupported Network	2
Virus Detection Event.....	2
How to access the service	3
Exclusions	3
Requirements and Assumptions	3
Supporting Services and Dependencies.....	4
Additional Services available for a charge.....	4
Document Control	5

Service Overview and Benefits

An Anti-Virus product is a programme which is designed to detect and remove malicious software including viruses from your computer. Malicious software, also known as malware, is computer software which can harm your computer systems and the software that you have installed on them. Unfortunately, malicious software can find its way into your computer via various means such as, email attachment, downloading across the internet, visiting a malicious website, or by inserting infected media such as a USB stick, mobile phone or CD/DVD.

Cyber threats are a reality for schools and having a defence mechanism in place to protect against those threats is key to protecting the ICT Infrastructure of a modern school. The security of your computer systems should be a multilayer approach such as by having an appropriate firewall installed, web filtering and regular software updates, Anti-Virus helps to secure your device should malicious software find its way in.

Service Description

This service provides McAfee Anti-Virus licences for all computers in a subscribing school, along with relevant virus definition dates and software upgrades.

Whilst the service still provides the above benefit, the service operates slightly differently depending on your school's individual circumstances, please see the description below which best describes your school.

Note: Where there are two networks in school (commonly Admin and Curriculum) but only one is supported by ICT & Digital, the relevant approach, as detailed above will be taken.

Supported Network

Definition: A supported network is either an admin, curriculum, or flat network for which an appropriate support SLA has been entered into with ICT & Digital.

In this scenario we will:

- Install, configure, and manage the Anti-Virus software on all supported servers.
- Install, configure, and manage the Anti-Virus software on all machines within the domain.
- Provide connection to a centralised management console (known as ePO) which provides reports and enables ICT & Digital to manage centrally the Anti-Virus software on installed machines reducing the need for support staff to visit machines to deal with problems.
- Ensure that Coventry City Council defined policies, relating to the installation and configuration of the Anti-Virus products are deployed to devices to ensure that the AV product does not cause any undesirable operation to software commonly used in schools such as SIMS, Solus, FMS, door entry systems etc are deployed.
- Manage upgrades to latest versions of the Anti-Virus engine software.
- Provide Anti-Virus agents for supported versions of Microsoft Windows, Apple Mac OS and Linux distributions.
- Provide upgrades to the Virus definitions which are used in detection (an active internet connection is required).

ICT & Digital staff regularly monitor the central server for notification of common threats and virus events across the school estate, where high priority threats are detected we will contact affected schools and advise on remedial action.

Virus Detection Event

Where a virus is detected, a call should be raised with our Service Desk who will assign the call as a P2. ICT & Digital staff will then advise on next steps to clean up and remove the malicious software.

Unsupported Network

Definition: An unsupported network is a network not supported by ICT & Digital.

In this scenario upon request we will:

- Provide access to the Anti-Virus software and installation instructions to school appointed technicians.
- Provide access to regularly updated versions of the Anti-Virus engine.
- Provide Anti-Virus agents for supported versions of Microsoft Windows, Apple Mac OS and Linux distributions.
- Provide upgrades to the Virus definitions which are used in detection (an active internet connection is required). (Provided automatically, via McAfee central repository)

Virus Detection Event

Where a virus is detected, school in the first instance contact their third-party support provider to obtain advice on how to proceed. Where the third-party support provider is unable to support, a call can be raised with ICT & Digital via our Service Desk for chargeable support.

How to access the service

Documentation on how to access this service can be found on our website at www.coventry.gov.uk/schoolsict or you can contact our service desk and raise a Service Request.

Exclusions

The following exclusions apply:

Area	Item Excluded
Non-Supported Equipment	<ul style="list-style-type: none">▪ Virus removal and investigation on non-supported equipment. This is available for an additional charge.
Non-Supported Operating Systems	<ul style="list-style-type: none">▪ Anti-Virus agents on non-supported operating systems. Supported operating systems are listed above.
Proactive Monitoring	<ul style="list-style-type: none">▪ We do not proactively monitor virus detection events within schools. Schools staff should contact ICT & Digital where appropriate for each virus detection event.

Requirements and Assumptions

To provide this service, we make the following assumptions.

- Adequate backups of sensitive data are being performed and checked.
- Laptops are regularly connected to the school network to receive their updates.
- Care should be taken when using removable media such as USB sticks, CDs, DVDs etc and these devices should be virus scanned before their contents is accessed.
- Care should be taken when accessing the internet not to download malicious software and when using email or file sharing services.
- Each member of staff knows how to perform a manual virus scan.
- You have familiarised yourself with the ICT Security Content available on our website https://www.coventry.gov.uk/info/186/ict/2366/ict_security_for_schools

Supporting Services and Dependencies

The following services support the operation of this service:

Service	Description
Admin Server Support	Your admin server supports the running of your school's administration network, it holds your files, manages printing, and contains your SIMS 7 databases (pupil database, solus upgrades database, FMS database and SIMS Discover). The Admin Server support service provides support for your admin server, its setup and configuration and operating system.
ISP Service (Internet Access)	The ISP Service provided by the City Council allows supported devices to receive their policy and anti-virus software updates.
Safe Data Remote Backup Service	Your data is valuable and should be protected. That is why we provide access to a remote data backup service which will backup and protect your schools most important data such as your school generated files and SIMS and FMS databases. Data is backed up off site to a secure data centre providing protection against, loss, malicious damage, fire, and flood.
Workstation Support	Where a workstation is covered for support, and a virus is detected no additional charge will be made to fix that machine.

Additional Services available for a charge

To compliment this service, we can offer the following additional services, which are available for a charge. The below services will be charged on a per hour basis.

Area	Description
Workstation Recovery	Where a virus or malware attack has resulted in the need to rebuild a workstation and if workstation cover is not already in place on that workstation, we are able to provide a service to reinstall and reload your software.

Document Control

The table below shows the changes to this document.

Version	Date Released	Change Notice	Pages Affected	Remarks
1.0	April 2021	New Document	All	New document format.
1.1	February 2022	New SLA Year	All	General updates and content review.