Microsoft Defender Antivirus FAQ

Lancashire County Council | EDUCATION DIGITAL SERVICES

What is Microsoft Defender Antivirus?

Microsoft Defender Antivirus is built into all modern Windows operating systems. It provides a fit for purpose threat management solution for school devices, blocking a wide range of viruses and malware, and frequently updates directly from Microsoft. It uses a range of techniques to ensure that only trusted files originating from the Internet can run. Microsoft Defender Antivirus provides:

- **Real-time protection** against viruses, malware, spyware, and other threats.
- **Cloud-delivered protection for faster detection of emerging threats.**
- **Behaviour-based, heuristic detection** to identify suspicious activity.
- **Automatic updates** for threat definitions and engine improvements.
- **Ransomware protection** for your most valuable folders

When do we move to Microsoft Defender Antivirus?

All schools must fully transition away from Sophos Intercept X – if purchased through Education Digital Services - by **13 March 2026** to allow sufficient time before the service ends on **31 March 2026**. Sophos Central and Intercept X will **cease on 1 April 2026** and will no longer be supported as part of our Broadband and Online Service Bundle.

What You Can Expect Next:

- **Migration Support Materials:** We will signpost to help schools prepare for and implement the switch. We will also provide template group policies and scripts if you wish to use our default configuration as a starting point.
- **Planning Ahead:** We recommend schools begin reviewing their current antivirus setup and preparing for the transition early to avoid last-minute disruption.
- **Licensing Timeline:** Your current Sophos Central and Intercept X subscription remains active until 31st March 2026.

How do we migrate to Microsoft Defender Antivirus?

We have prepared a comprehensive migration guide to support you, along with pre-configured settings templates that can be easily imported. These can be accessed via our website or the **Education Digital Hub**.

This guide should be shared with your Technical Support team to facilitate a smooth transition. Additionally, we offer an optional, chargeable service to assist schools with the migration process if required. To request a quote, please email educationprojects@lancashire.gov.uk.

Why are LCC moving away from Sophos Central and Intercept X?

Education Digital Services are continually working to reduce the costs associated with delivering school Broadband services. One of our latest steps in this effort is the replacement of Sophos Central and Intercept X with Microsoft Defender Antivirus. This change enables us to contain rising costs and offer schools a more competitive Broadband package.

Microsoft Defender Antivirus FAQ

Lancashire County Council | EDUCATION DIGITAL SERVICES

While this transition does reduce our overall service delivery costs, it's important to note that antivirus licensing is just one component of the total Broadband service cost. Due to inflation and other operational factors, the overall price to schools cannot be confirmed at this stage.

Microsoft Defender Antivirus has significantly evolved in recent years and now offers protection that is comparable to Sophos. Independent testing by AV-Comparatives and AV-TEST in 2025 confirms that Defender provides excellent real-time protection, low system impact, and strong malware detection capabilities. It is also integrated natively into Windows, reducing complexity and cost for schools.

This strategic move ensures schools continue to receive robust antivirus protection while helping us maintain affordability and sustainability across our service offerings.

Can we still use Sophos Central and Intercept X?

If your school wishes to continue using Sophos Central and Intercept X independently, we can support the transfer of your sub-estate to a third-party supplier. Please let us know once you've identified a suitable provider, and when you will have a licencing agreement in place with them and we will initiate the transfer process. We will notify Sophos that we authorise your sub-estate to be unlinked from our management and Sophos will be in contact with you to action the transfer. This process should not require any reinstallation of software on your devices and your configuration should remain the same. We recommend coordinating timelines with your new provider and completing the transfer by **13 March 2026** to allow sufficient time before the service ends on **31 March 2026**. All schools must fully transition away from Sophos Central and Intercept X (if purchased through Education Digital Services) before **31 March 2026,** as **all Sophos accounts will be deleted on 1 April 2026**.

As a reminder, your current subscription remains active until 31st March 2026 and will become unlicensed as of 1st April 2026.

How is Microsoft Defender Antivirus different from Sophos Central and Intercept X?

Both Microsoft Defender Antivirus and Sophos Central are high quality security suites, utilising a range of techniques to identify known malware and to identify if programs are behaving unusually.

	Microsoft Defender Antivirus	Sophos Intercept X
Installation	Built into each operating system	Requires additional installation of software
Update methods	Windows Update and from Microsoft security platform	Via Sophos endpoints
Configuration methods	On-device, Group policy, and Intune	Via Sophos Central web portal
Reporting	In-app, via event viewer	Via Sophos Central web portal

Microsoft Defender Antivirus FAQ

Lancashire County Council | EDUCATION DIGITAL SERVICES

Can you provide a comparison between Microsoft Defender Antivirus and Intercept X?

We are unable to provide such a document. However, please view the following links to compare yourself:

- **Sophos Central and Intercept X:** Sophos Endpoint powered by Intercept X
- **Microsoft Defender Antivirus:** Microsoft Defender Antivirus in Windows Overview - Microsoft Defender for Endpoint | Microsoft Learn

Is there a way of uninstalling Sophos from multiple devices in bulk?

If you are using a Windows domain or Intune to manage your Windows computers, you can use policies to trigger Sophos uninstallation on client devices.

Alternatively, **Sophos Central** allows you to select one or more devices, disable **Tamper Protection** and uninstall **Intercept X** from them. This action disables Sophos as the active threat protection software but does not remove all Sophos Central components from the device. The remaining components can be removed manually via the **Add/Remove Programs** feature on the device.

Do we need to do anything with Mac or Apple devices?

As per the recommendations from the National Cyber Security Centre (Antivirus and other security software - NCSC.GOV.UK), Mac and Apple devices both have their own inbuilt protections and typically do not require additional protection. The sandboxing approach to app use on iPads restricts the effectiveness of AV products, and MacOS uses Xprotect to secure the platform.

How does Defender stay up to date?

Microsoft Defender obtains product and signature updates through Windows Update. Product updates are issued monthly, and signature updates are released several times per day.

What level of support are LCC providing for Microsoft Defender Antivirus?

The support provided for a device depends on the subscribed services that apply to that device, namely:

- SIMS support service
- Technical Support for Curriculum Networks

Issues with Microsoft Defender Antivirus on these devices can be logged with our Service Centre. The level of support provided can be found within the Service Descriptions for these services.

Microsoft Defender Antivirus FAQ

Lancashire County Council | EDUCATION DIGITAL SERVICES

What is Microsoft Defender for Endpoint (MDE)?

Microsoft Defender for Endpoint is the next level of protection within the Microsoft Defender family. This provides a range of enhancements on Defender Antivirus itself, including:

- Central management console
- Emailed notifications to support staff
- Integration with Intune for schools that are cloud managed
- Attack surface reduction rules (mitigations performed on-device)
- Application and device control

Although Microsoft Defender for Endpoint is not part of our project at this stage, you can still access this enhanced functionality if your school has a qualifying Microsoft EES agreement (such as our Microsoft Annual Licensing service).

Microsoft Defender for Endpoint is provided for faculty devices within our Microsoft Annual Licencing Service. Client devices and server devices require additional licencing.

Please note that our future direction for schools over the next several years is to migrate from on-premise servers to fully cloud-based management. Microsoft Defender for Endpoint should be considered as part of the large feature set available within our Microsoft Annual licencing service and is the solution we are adopting for our Could Schools service.

Lancashire County Council Education Digital Services