Dealing with students' virus-infected PCs, laptops and other devices

Virus-infected devices pose a threat to network security and may adversely affect other users.

This process outlines how the IT Service Desk deals with personal devices owned by undergraduate, taught and research post-graduate students. These steps help to secure the University's wireless network and to help safeguard our wireless community from the threat of virus attacks.

If we detect that you have an infected device, we will follow these steps:

1. **We will immediately block your access** to our wireless networks.

2. IT Services will raise a Service Desk call and will notify you that:

   – your access to the wireless networks has been blocked due to a virus infection

   – your userID is blocked, meaning that none of your devices can connect to our wireless services

   – your access will not be restored until you can demonstrate that your device is clean and virus free

   – you will continue to have access to e-mail and other online resources on PCs in classrooms and study places.

3. **You must act to remove the infection** from your device.

   – you should either clean the infected machine yourself or seek commercial assistance; see www.abdn.ac.uk/it/student/help/laptop-support

   – you must ensure that a suitable virus protection package is installed as part of the clean-up process; see www.abdn.ac.uk/it/student/help/it-security

   – you must ensure that any memory sticks or other removable media you have connected to the infected device are also checked and, if necessary, cleaned.

4. Once you believe that your device is virus/infection free, you must **bring it to the Service Desk** for testing.

5. If your device is clean, your network access will be partially restored.

   – In order that we can be reasonably sure that your device will not become re-infected and cause further issues, your access to the wireless network will be restricted for a limited period; this will allow you to continue your academic work but will restrict other activities.

   – Full access will be restored when we are confident that your device is no longer a threat to the wireless network.