



Contents

P.2 Bring Your Own Device Policy

P.11 Instructions to connect to the Wi-Fi



THE NOBEL SCHOOL

DOCUMENT REFERENCE	Bring Your Own Device (BYOD) Policy
PUBLICATION DATE	September 2021
AUTHORISING OFFICER	Martyn Henson
AUTHORISING OFFICER'S SIGNATURE	
DATE APPROVED BY GOVERNORS	15/09/2021
AUTHORISING GOVERNOR'S SIGNATURE	
AUTHOR/EDITOR	Mark Smith
POST	Network Manager
REVIEW DATE	September 2023
TARGET AUDIENCE	Students
STATUS	Pending Approval

1. About this policy
2. Rules for connecting a device
3. Connecting devices to our system
4. Monitoring
5. Consequences for misuse
6. Disclaimer
7. Bring your own device agreement

Appendix: Acceptable Use Policy

1. About this Policy

The Nobel School recognises that many students have personal laptops or tablets. We understand that there are benefits to learning by offering students the opportunity to use personal ICT devices in school to support their learning. It is the intention of this policy to facilitate and support the use of personal ICT devices in school.

Students are expected to use personal ICT devices in accordance with this policy and by using any such device in school students agree to be bound by the additional requirements set out in this policy.

- The use of personal ICT devices falls under The Nobel School's Internet Acceptable Use policy (please see section 6 for a copy of this), which all students must agree to before they are allowed access to the internet.
- The purpose of allowing personal devices within school is entirely educational. Use of them for activities that are not related to education is prohibited.

Within this policy the term 'Device' refers to a laptop or tablet, such as an iPad. Within this policy, we may use the term 'BYOD', which means 'bring your own device'.

This policy currently applies to sixth form students, although in exceptional circumstances students in other year groups may be allowed to have their personal device connected to the school network.

2. Rules for connecting a device

- The use of a personal device should not be a distraction in any way to staff or students. Devices should be used purely for educational purposes and must not disrupt class or private study. Non-academic activities such as social media or games are not permitted.
- Devices must be checked regularly to ensure they are free from viruses and that they have up to date antivirus software on them.
- Devices must be checked regularly to ensure they are free from defects that would be classed as a health and safety risk. Any devices with obvious health and safety defects should not be brought in.
- Students must not use their device to record either audio or video, nor take photographs of other students or members of staff without their permission. Where consent is given, such media should never be uploaded or shared online. There are a number of occasions where parents or guardians may have indicated that pictures of their son or daughter should not be taken and/ or where, by doing so, a student's well-being or safety may be put at risk.
- If a member of staff requests that a personal device is put away or turned off, students must respect that decision.

3. Connecting Devices to our system

Either a students' Head of Year or the Assistant Headteacher (KS5) must approve connecting devices. We are also unable to connect devices without a signed consent and agreement form.

The Nobel School will provide instructions on how to connect to the school Wi-Fi. In the event that a personal device will not connect, we are unable to provide technical support to resolve any issues and are under no obligation to modify our network to help resolve it. Students will be limited to connecting one device to our WiFi.

To connect to our wireless system, you will need to install or trust two certificates on your personal device. The Nobel School is not able to assist in the installation of these certificates, but general guidance will be provided for a range of devices.

4. Monitoring

The school reserves the right to monitor and intercept traffic from of all student devices whilst connected to school systems. We may also maintain logs of websites visited whilst a student's personal device is connected to our network.

5. Consequences for Misuse

By using our network you agree to this policy and The Nobel School Acceptable Use policy. If we discover misuse of the device within school, your internet access may be revoked on your personal device and you may lose the right to bring it in. Where more serious misuse occurs, sanctions will be imposed as per our Behaviour and Acceptable Use policies.

6. Disclaimer

The Nobel School is in no way responsible for and accepts no liability for the following:

- Loss, damage to or theft of any personal device whilst in school, during school sponsored activities or whilst in transit to and from school. We are not responsible for any associated costs that may arise due to this.
- Loss or corruption of data on your personal device whilst connected to our network. Please ensure you keep copies of data elsewhere to ensure you have a backup of important data.
- Maintenance or upkeep of any device. We are unable to provide technical support for personal devices.
- Any issues or damage caused by the installation of the certificates required to connect to our Wi-Fi.

BYOD is not a compulsory part of a student's education. As such, the decision to bring a personal device in to school rests solely with the student and their parent(s) or guardians(s).

Parents or guardians should ensure that a suitable private insurance is in place to cover loss or damage.

7. Bring your own device agreement

I wish to use my personal device for learning whilst at the Nobel School and confirm that I understand and agree to the following:

- I have read, understood and agree to all of the terms contained within the **Bring your own device policy** and the **Acceptable use policy**.
- I understand that the terms of this policy will apply at all times, both during the school day and outside school hours, whilst on the school site.
- I understand that The Nobel School in its discretion may amend, or remove this policy at any times and I will be bound by the terms of the policy as amended.

Parents/ guardians and students – Please complete this acknowledgement form agreeing to the content of this policy. Students will be unable to use their own device in school unless both parties agree to the contents of this policy.

As a student, I understand and agree to the conditions set out in the above BYOD Policy as well as the Acceptable Use policy. I understand that if I breach this policy then I will lose the privilege of bringing my own device in and that I may face other sanctions.

Student Name

Form Group

Signed (Student)

Date

As a parent/ guardian, I understand and agree that my child will be responsible for adhering to this policy. I have read and understood this policy with my child and they understand the trust and responsibility required for having their own device in school. I acknowledge that The Nobel School accepts no liability for personal devices as set out in section 6 of this policy.

Parent/ Guardian Name

Signed (Parent/ Guardian)

Date

Appendix: Acceptable use policy

The school has provided computers and some iPads for use by students. They offer access to a vast amount of information for use in studies, with the internet and programs offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all students, who are encouraged to use and enjoy these resources, and ensure they remain available to all. Pupils are responsible for good behaviour on the Internet just as they are in a classroom or a school corridor. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

Equipment

- Do not attempt to install or store programs of any type on the computers without permission.
- Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
- Do not use the computers for commercial purposes, e.g. buying or selling goods.
- Do not copy personal files on to the network. These may be deleted without warning.

Security and Privacy

- Do not disclose your password to others, or use passwords intended for the use of others. Respect the privacy of other's at all times.
- Never tell anyone you meet on the Internet your home address, your telephone number, your school's name, or send them your picture.
- Respect, and do not attempt to bypass, security in place on the computers, or attempt to alter the settings.
- Staff may review files and emails to ensure that users are using the system responsibly. You must not keep inappropriate files or pictures in your network area.
- Do not let anyone else use your school swipe card. You are responsible for all activity on the card. If the card is lost or stolen you must report this immediately to the IT Office. You will be charged for a new card.

Internet

- Do not access the Internet unless for study or for school authorised/supervised activities. Random checking of internet use will take place regularly to monitor e-safety and appropriate usage.
- Do not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.

- Do not attempt to access social media or access chat rooms over the Internet. This takes up valuable resources which could be used by others to benefit their studies.
- Never arrange to meet anyone unless your parent/guardian or teacher goes with you. People you contact online are not always who they seem.

Email

- The school provides you with a school email address, which should be used for school work only. You need to be aware a copy of all emails sent to and from students is automatically kept and can be accessed by the System Administrator should the need arise. This is for your own safety.
- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is not allowed.
- Never open attachments to emails unless they come from someone you already know and trust. They could contain viruses or other programs which would destroy all the information and software on your computer.
- The sending or receiving of email containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content. Always report such messages to a member of staff.

Media and Social Networking

- Except when it is part of a planned teaching and learning experience involving the full permission of those involved, it is completely prohibited to take any video or photographs of students or staff within the school context. There are a number of occasions where parents may have indicated that pictures of their sons or daughters should not be taken and or where, by doing so a student's well-being or safety may be put at risk.
- If any such files are shared through mobile phones, computers or uploaded to social networking sites, the school will work with the police under the misuse of telecoms act. The school would treat very seriously any misuse of the described media. Anyone found guilty of this offence will face possible permanent exclusion or dismissal.
- Social Networking Sites should not be used in school. All networking sites should be blocked, if they are not please inform one of the IT Technicians immediately. Anyone found on a social networking site will have their internet access removed immediately. This will impact your ability to do your school work.
- A wide variety of technological resources are provided in school to enhance the learning experience for students and to ensure that the most up to date facilities are experienced as part of your education. These facilities are only to be used within planned activities with staff and school knowledge. We expect you to exercise good judgement in the way that you engage with all new technologies, to ensure the integrity of the school and other student's safety.

Important: Use of bad language and abuse of other people online, including bullying or racist remarks, comes under the Misuse of the Telecommunications Act 1984 and is an

arrestable offence. Please do not put yourself in a position of vulnerability. You must understand that once you have committed information to the internet, it is there forever. Anyone found posting disrespectful comments about anyone in school, brings the school into disrepute and the school takes this very seriously. We may involve legal and/or police engagement if necessary to resolve such issues.

Please read this document carefully. Only once it has been agreed to will access to the school computers and the internet be permitted. If any student violates these provisions, access to the Internet will be denied and the student will be subject to disciplinary action.

Additional action may be taken by the school in line with existing policy regarding school behaviour. For serious violations, suspension or expulsion may be imposed. Where appropriate, police may be involved or other legal action taken.

Under the Data Protection Act, the school has a responsibility to ensure the safeguarding of student information. Any students found in a staff user area will face very serious consequences, which may include exclusion and/or prosecution.



Nobel

Connecting to the Wi-Fi (student user)

Steps to take at home

In order to connect to the school's Wi-Fi you will need to install a certificate on the device you wish to use. Without this, the internet will not work in school. The link for the instructions is below:

<https://www.rm.com/products/rm-safetynet/ssl-interception>

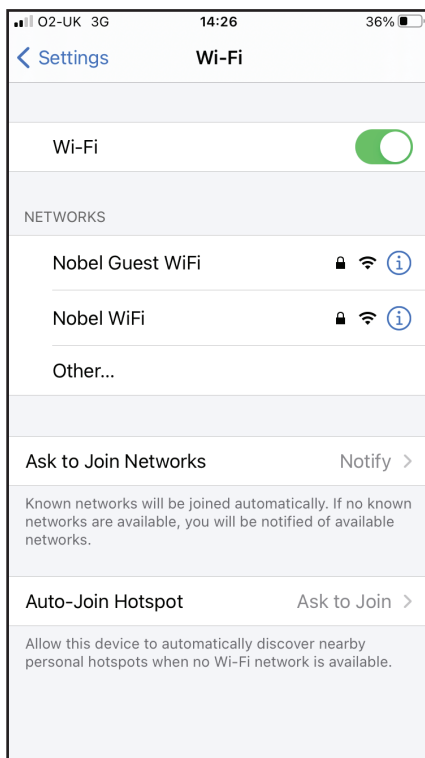
You will need to scroll down to **Downloads** and select the type of device you have. When given the option of Managed or Standalone, make sure you select Standalone and follow the relevant instructions.

Connecting to the Wi-Fi

Please follow the specific instructions for the type of device you have. You will not be able to connect until you have returned a signed form to IT.

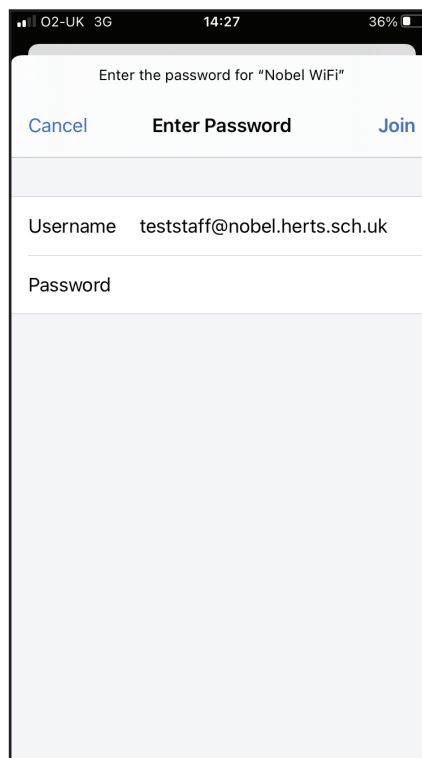
Apple iOS

1.



Select **Nobel WiFi** from the list of available networks.

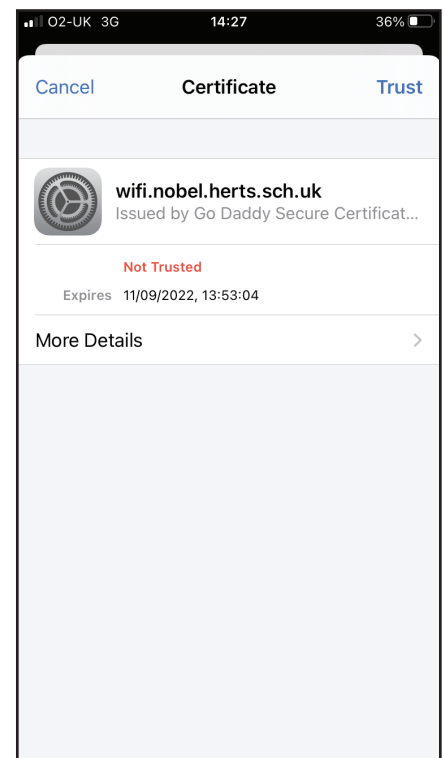
2.



You will be prompted to enter a username and password. This is your email address and password.

Once filled in, press **Join**.

3.



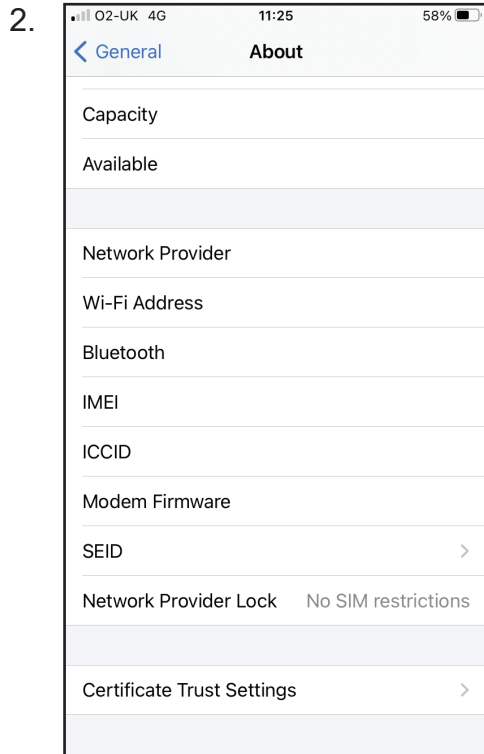
You will then be prompted to trust a certificate with the name **wifi.nobel.herts.sch.uk**.

Press **Trust**.

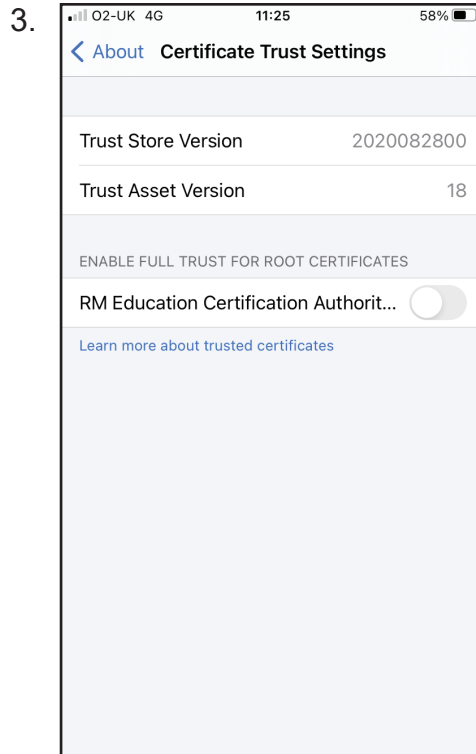
MacOS devices should be similar, except it will ask you to install the certificate rather than trust it.

Apple iOS trusting the certificate

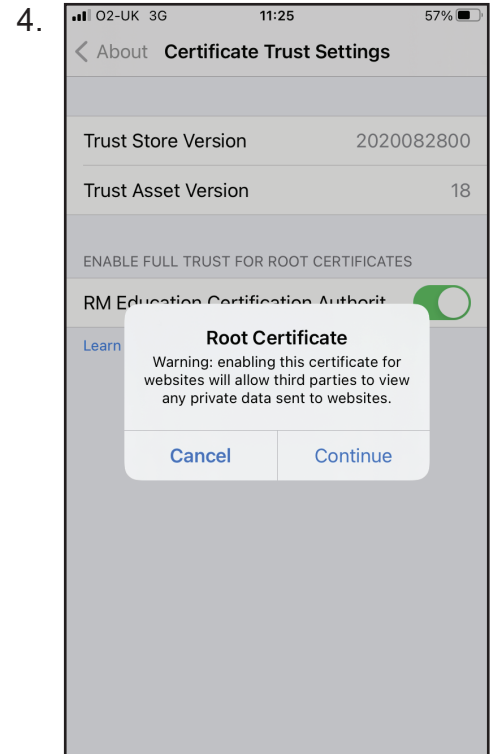
1. On later versions of iOS, you must trust the certificate manually when you install a profile that has been downloaded from a website.



Go to **Settings > General > About** and at the bottom press **Certificate Trust Settings**.



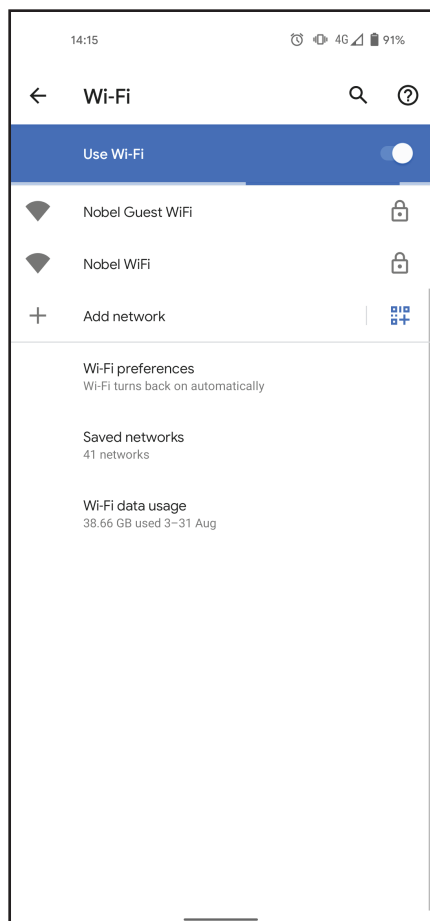
Under the heading **Enable full trust for root certificate**, enable the **RM Education Certification Authority**.



You will then be prompted to confirm. Press **Continue**.

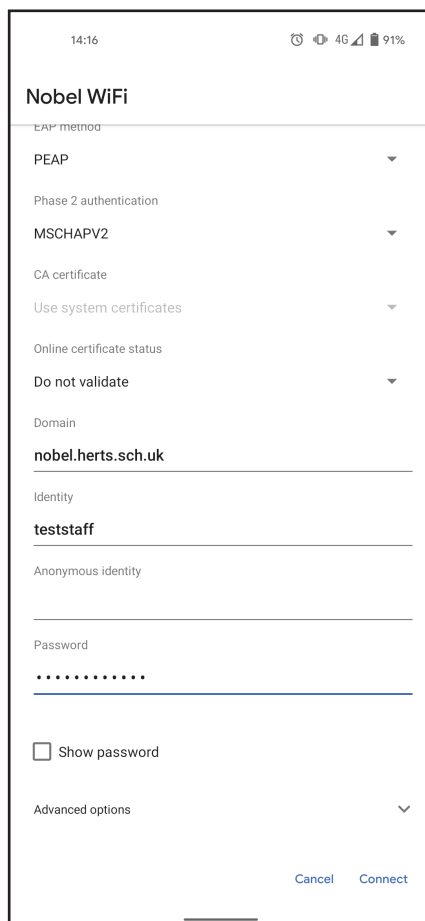
Android

1.



Select **Nobel WiFi** from the list of available networks.

2.



Every version of android is different and so your view may not be the same as this.

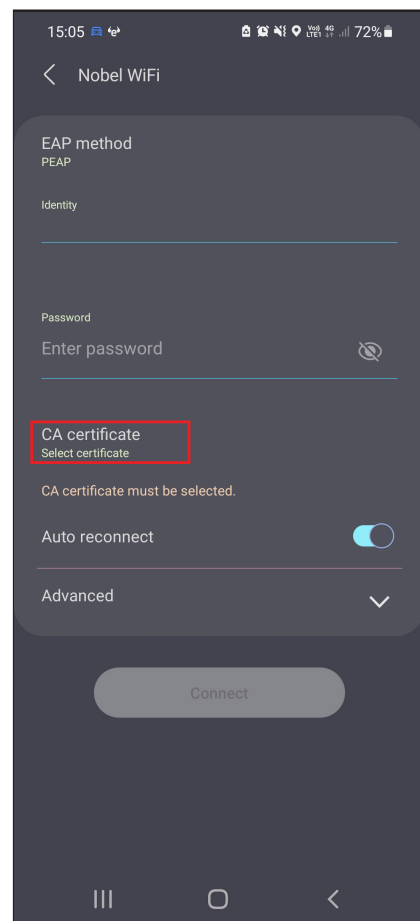
You will need to enter the following information:

Domain
nobel.herts.sch.uk

Identity
your username that you sign in to a school PC with

Password
Your password

3.



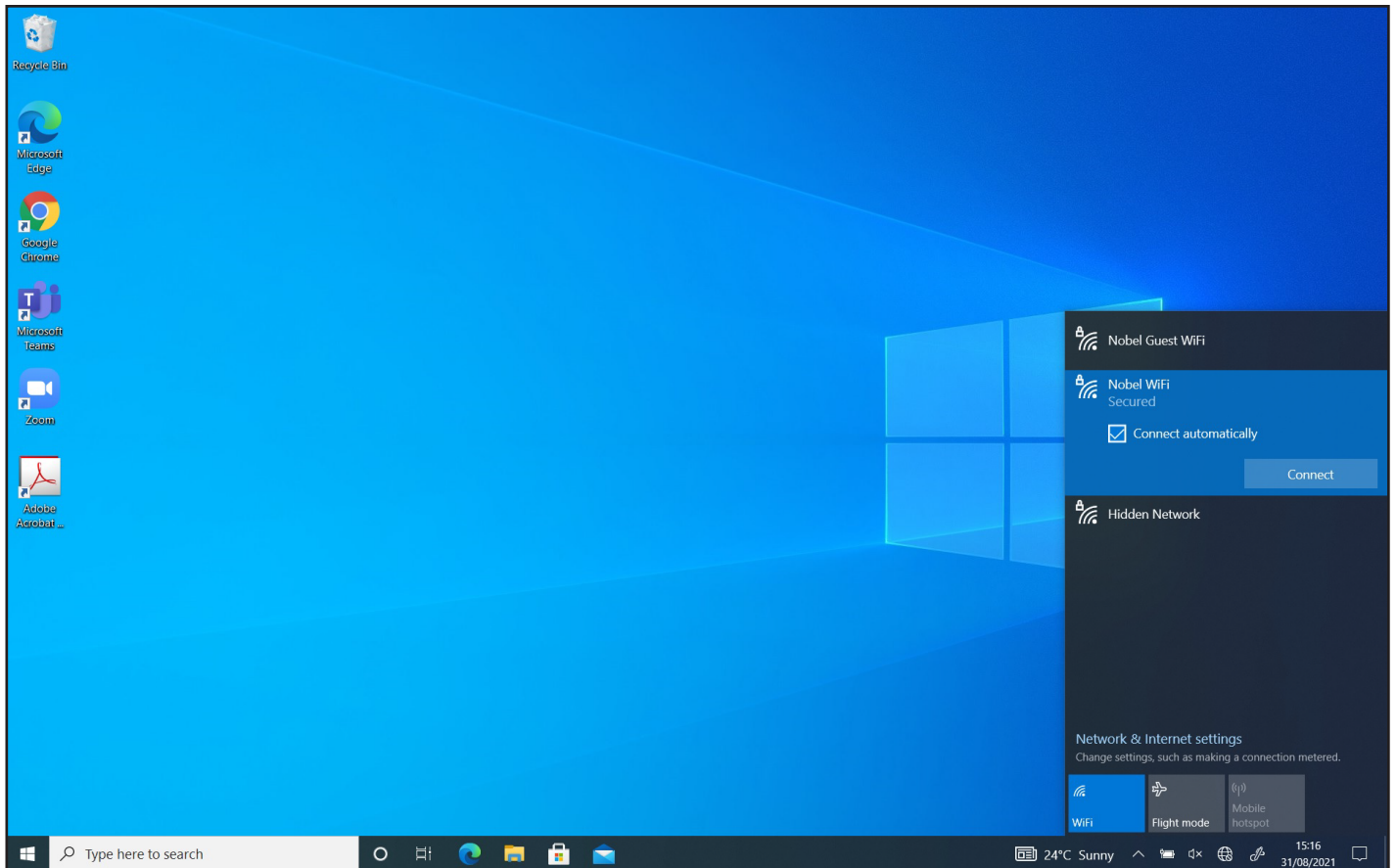
On some versions of Android the **Domain** field may not be visible. Press the field **CA Certificate**.

Select **Use system certificates** on the list that opens.

Following this, the **Domain** field to show.

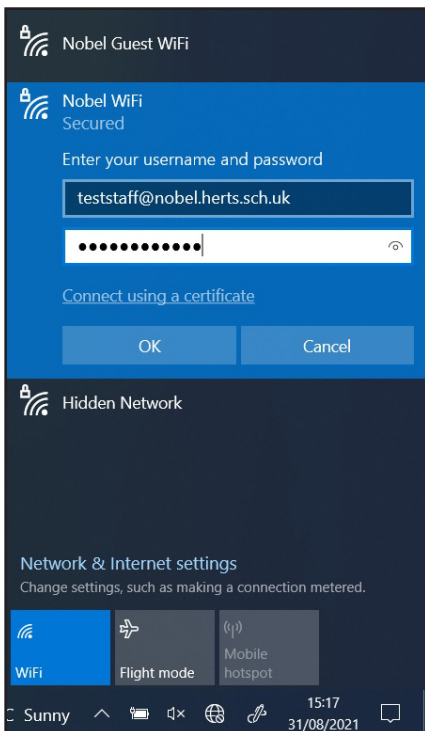
Windows

1.



Select **Nobel WiFi** from the list of available networks. If **Connect Automatically** is not ticked, tick it and click **Connect**.

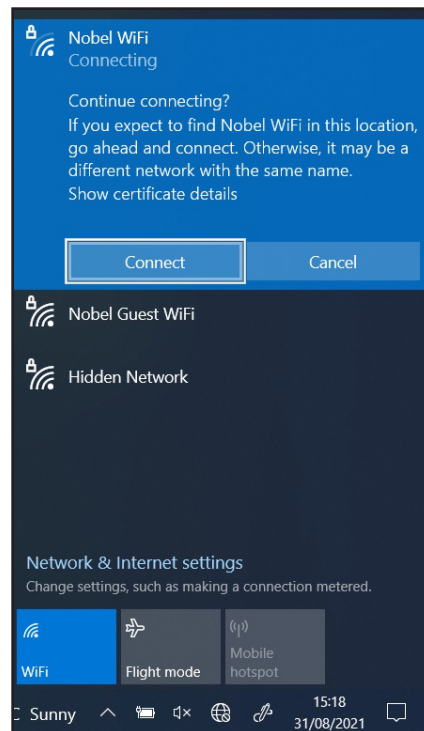
2.



You will be prompted to enter a username and password. This is your email address and password.

Once filled in, press **OK**.

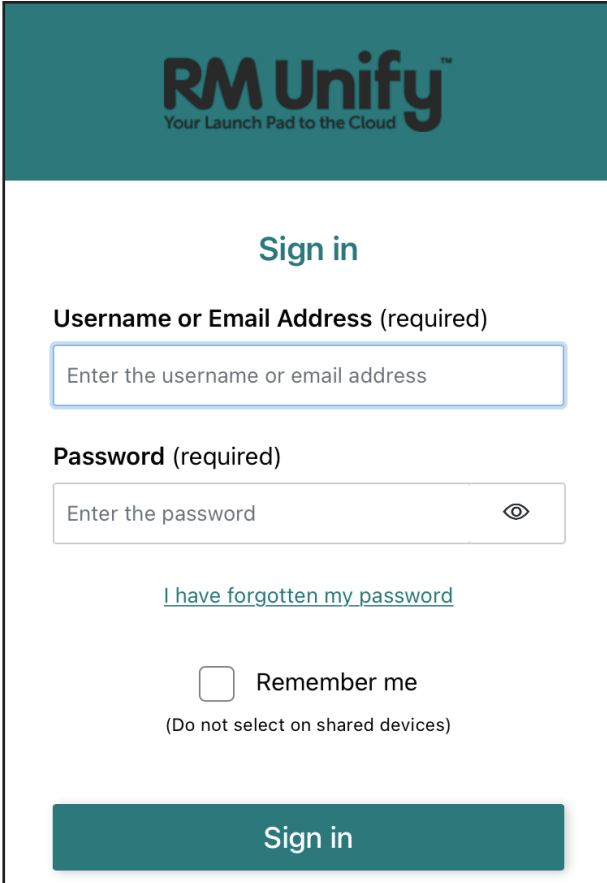
3.



If you get asked to continue connecting, select **Connect**.

Daily Sign in

1.

The image shows a web browser window displaying the RM Unify sign-in page. At the top is a teal header with the 'RM Unify' logo and the tagline 'Your Launch Pad to the Cloud'. Below the header, the page has a white background. The title 'Sign in' is centered in teal. Underneath, there are two required fields: 'Username or Email Address' and 'Password'. The first field is a light blue box with the placeholder text 'Enter the username or email address'. The second field is a light grey box with the placeholder text 'Enter the password' and a small eye icon to its right. Below the password field is a teal link that says 'I have forgotten my password'. Further down is a checkbox labeled 'Remember me' with the text '(Do not select on shared devices)' below it. At the bottom of the form is a large teal button with the text 'Sign in' in white.

Once connected, when you open a web browser and try and view a webpage you may initially be asked to sign in on the RM Unify webpage. This should occur once per day.

You will be prompted to enter a username and password.

This is your email address and password.

If you wish, you can tick remember me to speed up login.

You will then be directed to the page you were trying to access.

2. Some devices may not prompt you to sign in to RM Unify as they are automatically able to send the login details to the site. If this is the case you will not have to complete the previous step and will just be able to browse the internet as normal.