The internet is an invaluable resource for learning, teaching, and day-to-day operations. A safe, filtered internet connection is provided by the school for this purpose.

- Internet access provided by the Trust/school is not private. The Trust/school monitors and filters internet usage to improve delivery of service and to safeguard its community of users.

- Any access to the internet from the network can be traced to the Trust/school. You must not use the internet in any way that might bring the Trust/school into disrepute.

- Incidental personal use of the internet is permitted if usage is limited to a reasonable amount and does not interfere with your learning.

- If, as part of your incidental personal use of the internet you are required to provide an email address, you should use a personal email and not use your school email address.

- Use of the Trust/

Access to systems and data are provided to you for the purposes of learning, teaching, and day-to-day operations.

- You may only access information on Trust/school systems if you have been properly authorised to do so and if you need the information for learning.
- Unauthorised access to or modification of data is a criminal offence under the Computers' Misuse Act 1990.
- Illegal activities of any kind are strictly forbidden. Any illegal activities will be reported to the authorities.
- It is illegal to circumvent any access or authentication restrictions, or otherwise attempt to compromise the security of the   systems.
- You must not probe, scan, or test the vulnerability of any part of the   systems without proper authorisation.
- Activity that threatens the safety of the   ICT systems, or activity that attacks or corrupts other systems, is forbidden.
- If a virus is detected, you must report this to IT Services immediately.

- Users are expected to exercise good handling and care of all school-provided hardware and to maintain sound physical security of hardware they are using.
- You must be careful to prevent school-provided equipment from being lost or stolen.
- Any malicious attempt to harm or destroy any equipment or data will result in loss of access, disciplinary action such as exclusion and, if appropriate, legal referral.
- The use of software from unauthorised sources is prohibited.
- Memory sticks and other portable devices should never be used to transfer data to or from Trust/school. You should use OneDrive where possible to save data to the cloud instead. If you need to transfer data via another method, please contact IT Services for support.

- You may connect a personal mobile device to the

‹ Student-owned devices, including mobile phones, should not be used dur4

- When undertaking formal assessment, you must comply with guidance from the Joint Council of Qualifications and examining bodies relating to malpractice, including malpractice involving use of

- Generative AI can generate convincing content of all kinds including that which is potentially harmful, for example, highly credible scam emails requesting payment that are more authoritative and believable than seen previously. It is more important than ever that users are informed in cyber threats and can apply professional judgment to manage risk.

- You must not access or create harmful content through generative AI.

  (2023).

- You must not photograph or video other students or staff under any circumstance unless you have been specifically directed to do so by a member of staff.

- Photographs and videos taken at school (including events or trips held off-site) must never be posted on social media or shared with others via any other means.

- Under no circumstances should you share or upload staff pictures online.

- Any breach of these

- Some cases may result in more severe sanctions including the possibility of exclusion from school or in the case of illegal activities, referral to the relevant authorities or even criminal prosecution.

- All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

All users must adhere to the following password policy for all accounts used in conjunction with the Trust/school:

- We recommend a combination of unrelated words (known as a passphrase) which can be comprised of upper (A-Z) and lower (a-z) case, digits (0-9) and special characters for maximum strength (see below for examples).

- . We encourage you to adopt passphrases that are naturally more secure and easier to remember since they do not involve random numbers and special characters.

- * * * *

However, you must <u>not</u> use this same password for <u>any other service</u> irrespective of whether this service is for work use or personal use.

‹ .

‹ . Password managers are also permitted, however, please discuss this with IT Services to ensure the manager you are using is safe and secure.

‹ This includes IT Services. Never communicate passwords via email, telephone, Teams chat or any other means. Passwords should never be written down.

‹ (for example, .

‹ providing that it meets all the above criteria. If your password does not meet some or all the criteria above, please change your password immediately.

‹

Department for Education (2023)   available here.