WINCHESTER
COLLEGE

WINCHESTER COLLEGE IT SERVICES ACCEPTABLE USAGE POLICY

Reviewed:	September 2024
Next review date:	September 2025

1 - Online Behaviour

As a member of the school community, you should follow these principles in all your online activities.

- The school cannot guarantee the confidentiality of content created, shared and exchanged via school systems. Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example content that is obscene, or promotes violence, discrimination, or extremism, or raise safeguarding issues).
- Respect the privacy of others, do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without obtaining the relevant permission to do so.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage interfere with, or gain unauthorised access to the computer systems of others or carry out illegal activities.
- Staff should not use their personal email or social media accounts to contact pupil or parents, and pupils and parents should not attempt to discover/contact the personal email addresses or social media accounts of staff.

2 - Using the School's IT Systems

Whenever you use Winchester College IT systems (including be connecting your own device to the network) you should follow these principles:

- Only access school IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- The provision of Winchester College email accounts, WiFi and internet access is for official school business, administration and education. Staff and pupils should keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of these accounts. Again, please be aware of the school's right to monitor and access internet history and email use.

3 - Passwords

Passwords protect the school's network and computer system and are your responsibility. They should not be obvious (for example “password”, 123456, family name or birthday), and nor should they be the same as your widely used personal passwords.

You should not let anyone else know your password, nor keep a list of passwords where they may be accessed and must change it immediately if it appears to be compromised.

You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights. All the school accounts are protected with multi factor authentication (2FA).

4 - Use of Property

Any property belonging to the school should be treated with respect and care and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the IT department.

5 - Use of Personal Devices or Accounts and Remote Work

Pupils must use a Microsoft Surface Pro procured and managed by the IT department to do their schoolwork. Staff must use school issued devices (PCs, laptops, Microsoft Surface Pro, mobile phones etc) where issued, for official school business and must conduct all official school business on school systems. Staff must not use personal email accounts for school business.

The school does not generally allow the use of personal devices to conduct school business, other than to access web-based services (for example, Outlook, Teams). Staff should ensure that any personal or confidential school data downloaded onto their devices through accessing web-based services (for example, email attachments) is deleted once viewed.

Pupils and staff must obtain approval from the IT department for any use of personal devices for school purposes, including the removal of personal data or confidential information from school systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick.

Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the school's policies, including multi factor authentication and encryption and be kept up to date with the latest security releases and updates

6 - Monitoring and Access

Staff, parents and pupils should be aware that school email and internet usage is filtered and monitored for safeguarding, conduct and performance purposes. The school uses both device level and network level monitoring systems. The school may access both internet history and school email accounts where necessary for a lawful purpose, including serious conduct or welfare concerns, extremism and the protection of others.

Any personal devices used by pupils, whether or not such devices are permitted, may be confiscated and examined under such circumstances. The school may require staff to conduct searches of their personal accounts or devices if they were used for school business in contravention of this policy, and in particular if there is any reason to suspect illegal activity or any risk to the wellbeing of any person.

7 - Use of AI Technology

Any use of AI which is deemed to run counter to the principles laid out within this document, or that is found to be illegal or damaging to individuals or groups within our community, could be found to be in breach of this AUP and will be dealt with under the guidance for Winchester College's disciplinary policy.

8 - Compliance with School Policies

To the extent they are applicable to you, you will ensure that you comply with Winchester College's e-Safety policy, Safeguarding policy and other school policies in relation to your use of the school's IT systems.

9 - Breach Reporting

The law requires the school to notify personal data breaches, if they are likely to cause harm, to the authorities and in some cases to those affected. A personal data breach is a breach of security leading to the accidental or lawful destruction, loss alteration, unauthorised discloser of, or access, to personal data.

This will include almost any loss of or compromise to personal data held by the school regardless of whether the personal data falls into a third parties' hands. This would include:

- Loss of an unencrypted laptop, USB stick or a physical file containing personal data.
- Any external hacking of the school's systems, for example through malware.
- Application of the wrong privacy settings to online systems
- Misdirected post or email.
- Failing to BCC recipients of a mass mail.
- Insecure data disposal.

The school must generally report personal data breaches to the ICO without undue delay (**within 72 hours**), and certainly if it presents a risk to individuals. In addition, controller must notify individuals affected is that risk is high. In any event the school must keep a record of any personal data breaches regardless of whether we need to notify the ICO.

If pupils become aware of a suspected breach, they should contact their housemaster or tutor in the first instance. If staff become aware of a suspected breach, they should contact dataprotection@wincoll.ac.uk

Data breaches will happen to all organisations, but the school must take steps to ensure they are rare and limited as possible and that, when they do happen the worst effects are contained and mitigated.

This requires the involvement and support of all staff and pupils. The school's primary interest and responsibility is in protecting potential victims and having visibility of how effective its polices and training are. Accordingly falling victim to a data breach either by human error or malicious attack will not always be the result of a serious conduct issue or breach of policy but failure to report a breach will be a disciplinary offence.

10 - Breaches of this Policy

A deliberate breach of this policy by staff or pupils will be dealt with as a disciplinary matter using the school's applicable procedures. In addition, a deliberate breach by any person may result in the school restricting that person's access to the school IT systems.

If you became aware of a breach of this policy or the e-Safety policy, or you are concerned that a member of the school community is being harassed or harmed online you should report it to the Designated Safeguarding Lead. Reports will be treated in confidence wherever possible.

11 - Acceptance of this Policy

I understand and accept this acceptable use policy of Winchester College.