Information and Communication Technology Acceptable Use Policy

Ascham School

1. PURPOSE

The School's Information and Communication Technology (ICT) resources are intended for the benefit of staff, students, parents, and the wider Ascham community. Ascham requires that its ICT resources are used in a legal, ethical, and responsible manner and authorised users and their guardians are required to familiarise themselves with and accept the terms of the ICT Acceptable Use Policy (AUP). The ICT AUP outlines the requirements for:

- Acquiring ICT resources for the School.
- Providing ICT resources to staff, students, parents, and the Ascham community.
- The rights and responsibilities in relation to the use of IT resources.

2. BACKGROUND

Ascham provides computing, tablet device, networking, information and communication systems and resources to the Ascham community to support teaching and learning, administration, and other Ascham business. Access to ICT services is granted to authorised users that are members of the Ascham community and have accepted the terms of the ICT AUP.

3. SCOPE

This policy applies to all users of Ascham's ICT resources at all times, regardless of location (on or off campus) and whether such use occurs during or outside of school operating hours. The AUP also applies to anyone connecting personally owned equipment (e.g., laptops) to the Ascham network and to the use of data and information that may be accessed via Ascham's ICT resources.

4. DEFINITIONS

Artificial Intelligence (AI) – refers to an engineered system that generates predictive outputs such as content, forecasts, recommendations, or decisions for a given set of human-defined objectives or parameters without explicit programming. AI systems are designed to operate with varying levels of automation.

Authorised Purposes – means purposes associated with work or study at Ascham, provision of ICT services to or by Ascham, limited personal use, or any other authorised purpose.

Authorised User – general authorisation to use ICT Resources is granted upon enrolment, employment, official affiliation with Ascham, or as a member of the community that uses Ascham's services and facilities (e.g., Swim School or the Ascham Holiday Academy). Authorised users will need to obtain accounts and passwords (passphrases) to enable access to Ascham ICT resources. Authorised Users that are minors (Students) will require parent / guardian consent.

Cyber Bullying - the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature.

Cyber Safety - is the safe and responsible use of ICT resources; and in the Ascham context educating users on how to keep information safe and secure, about being responsible with the use of information, and being respectful of other people online.

Deepfake – a 'Deepfake' is a type of artificial intelligence used to create convincing images, audio, and video hoaxes. The term describes both the technology and the resulting bogus content.

Generative AI – means a type of AI that uses a process of machine learning to create new and original content, such as images, videos, or text. This is achieved through the use of deep neural networks that can learn from large datasets and generate new content that is similar to the data it has learned from.

ICT - Information and Communication Technology

ICT Resources – means all Information Communication Technology Resources and related physical resources provided by Ascham to assist or support teaching, learning, and administrative activities. This includes, but is not limited to, the use of:

- All computers, tablet devices and all associated data networks, internet access, email, hardware, data storage, computer accounts, all identity and access systems, media, software (both proprietary and those developed by Ascham) and telephony services.
- All physical spaces using information technology and designated for teaching, study, and administration.
- ICT services provided jointly, or by third parties that have been engaged by Ascham.
- Equipment owned or leased by users when used to connect to the Ascham networks or third-party services that have been engaged by the School.

Illegal Activity – means the creation, transmission, storage, downloading, or possession of any material that is defined as criminal, or pertaining to criminal activity in Australia.

Intellectual Property - refers to rights relating to confidential information, knowledge, creative ideas, documents, inventions; literary and artistic works; designs; and symbols, names and images.

Limited Personal Use – means use of ICT resources that is not for Ascham purposes, and is:

- Not for financial gain;
- Does not cause unreasonable burden on Ascham IT resources;
- Does not interfere with the execution of duties.

Multi Factor Authentication – known as 'MFA' or two-factor authentication (2FA) is way to strengthen ICT security by introducing an additional means of authenticating a user when logging on to hardware or software. It is considered best practice to have MFA for systems storing sensitive information.

Passphrase – is a stronger form of password that's used by Ascham for system authentication. A passphrase is a sequence of words or other text similar to a password in usage, but longer for added security.

Social Media - websites and applications that enable users to create and share content or to participate in social networking.

Staff – refers to all individuals employed by and contracted to work for Ascham. Staff may also refer to volunteers, interns, and teacher education or work experience students.

5. PRINCIPLES

a) ICT resources are core to Ascham's operations and support the Schools strategic initiatives under the Towards 2030 strategy.
b) Ascham IT will apply appropriate security measures and protections to its ICT resources in line with the Information Security Policy.

c) The acquisition and roll out of ICT capabilities and resources to support the School in responding to emerging needs will be streamlined wherever possible.
d) The risk from cyber security threats will be minimised and where appropriate aligned with business continuity planning and disaster recovery processes.
e) The School acknowledges that ICT resources may be unavailable from time to time for either planned or unforeseen circumstances.
f) All authorised users will be lawful, efficient, economical, and ethical in their use of Ascham's ICT resources. Authorised users, will as far as possible:
    - Respect the rights of all users;
    - Ensure ICT Resources and related physical resources are only used for purposes authorised by Ascham;
    - Ensure the security and integrity of ICT Resources; and
    - Ensure Ascham ICT Resources are used in a way which complies with all relevant laws, and contractual obligations governing the use of ICT Resources.

6. POLICY STATEMENTS

6.1. Acquisition and Provision of ICT Services

Ascham IT under the Director of ICT is responsible for:

a) Acquiring ICT resources directly.
b) Setting IT architecture standards, procedures and guidelines that must be adhered to for all ICT services.
c) Providing advice and due diligence for School ICT contracts and agreements.
d) All staff must seek advice and where appropriate approval when seeking to procure new ICT hardware and services.

6.2. Conditions of Use

It is a condition of access to Ascham's ICT resources that authorised users and / or their parent / guardians agree to comply with all the provisions of this Policy and understand that their actions and usage of Ascham's ICT resources may be monitored, and records retained.

- For staff, this includes the acceptable ICT guidelines outlined in Annex 1.
- For students and parents, Annex 2 and Annex 3 provide guidelines for student and parent acceptable ICT behaviours and form the basis for the ICT Acceptable Use forms that parents are required to accept on their daughters' behalf.

6.3. Access to ICT Resources

Authorisation to use ICT resources may be granted upon enrolment, employment, official affiliation with Ascham, or as a member of the community that uses Ascham's services and facilities (e.g., Swim School of the Ascham Holiday Academy). Staff and students are provided with the following:

a) Ascham email accounts
b) Access to collaborative technologies, shared mailboxes (where appropriate), specialised applications and other resources.
c) Access to necessary and appropriate information through storage systems, databases and other ICT resources.

It is important to note that email messages and files created and stored on the School network remain the property of Ascham. The School is the owner of all ICT resources it provides for staff and student use, including all information, intellectual property and content including files, documents, emails, attachments, text messages and electronic communications. Ascham is also the owner of all computer hardware, tablet devices, software, systems, network services, telephones, including mobiles, fax, and other communication devices procured by the School for use by staff and students.

Parents and guests to the School campus may connect to the Ascham WiFi network providing the member of staff hosting them authorises this via the ClearPass approval process.

Access to ICT resources outside the purposes of learning, teaching, administration, and other Ascham business, except for limited personal use, is unauthorised. Unauthorised access to ICT resources is a breach of the ICT Acceptable Use Policy.

Restrictions or conditions may apply to any person seeking authorisation to use Ascham ICT resources, including:

- The mandatory use of a username and passphrase (password), multifactor-authentication (where available) and / or another authentication method such as pin code, fingerprint, yubikey etc;
- Restrictions or conditions as to the facilities the person is authorised to use; and the data they are authorised to access.
- The provision of acknowledgment by the person to the effect that they will abide by this Policy and any applicable conditions of use, including:
    - Written acknowledgment signed by the user; and / or requirements that the Authorised User click on or enter an acknowledgment as a condition of access to any ICT Resources.

Authorised users will be asked periodically to renew their acceptance, particularly after major amendments to the policy. Students moving from Hillingdon to Fiona and from Fiona to Senior School will be asked to renew their acceptance of the policy. *Users who do not accept the ICT Acceptable Use Policy may not be granted access to the School's ICT resources or may have existing ICT resources withdrawn.*

Access to ICT resources may be restricted or withdrawn if there is reasonable suspicion or evidence of misuse of ICT resources, or a breach of any policy or applicable law.

6.4. Responsibilities of Authorised Users

Each Authorised User is responsible for:

- Usage of the unique computer accounts which Ascham has authorised for the user's benefit.
- Selecting and keeping a secure password/passphrase for each of these accounts, including not sharing passwords/passphrases, and logging off after using a computer.
- Using the ICT facilities in an ethical and lawful way, in accordance with Australian laws.
- Ensuring that except for limited personal use, ICT Resources are only used for authorised School purposes.

- Co-operating with other users of the ICT Resources to ensure fair and equitable access;
- Observing their obligations under this Acceptable Use Policy; staff are also required to observe their obligations under the Information Security and Data Governance Policies.
- Observing the Terms of Service or Acceptable Use policies of third-party products or services that have been engaged by Ascham.
- Users with BYO laptops (owned by either staff or students), phone or tablet devices may be required to install Ascham Antivirus and Firewall software before being granted access to Ascham ICT resources.

Authorised Users must not use the ICT resources:

- To abuse, vilify, bully, defame, harass, discriminate (by virtue of race, religion, national origin or other) or to create, send or receive offensive, obscene (pornographic) or illegal material.
- To spam; this includes sending unsolicited internal emails to staff or students.
- To impersonate, record, or unlawfully share personal data relating to another person. For example this includes but is not limited to signing a person up to websites or services, recording them without their knowledge or consent, or creating a deepfake to impersonate someone.
- To infringe the copyright or other intellectual property of another person or organisation.
- To disrupt the business operations of the School.
- To perform any other unlawful or inappropriate act.
- In such a way as to damage the reputation of Ascham or in a manner that may cause embarrassment to the School.

6.5. Misuse of ICT Resources

Misuse of Ascham's ICT resources is a breach of the ICT Acceptable Use Policy.

Any member of the Ascham community who becomes aware of possible misuse of an ICT Resource must report it to:

- Their manager or Head of Department;
- The Head of Human Resources;
- The Director ICT; or
- The Head of School.

Misuse of ICT resources could result in revocation of access to Ascham's ICT resources. Should misuse be determined, formal disciplinary action may occur, and Ascham may refer serious matters to the appropriate external authorities which could result in civil or criminal proceedings.

6.6. Liability

Ascham is not liable for loss, damage or consequential loss or damage arising directly or indirectly from the use or misuse of any ICT resources. This includes loss of data stored on any ICT resources and / or damage to equipment used in conjunction with any ICT resources.

6.7. Monitoring and Surveillance

All content on the Ascham network and stored within Ascham ICT resources is owned by the School and may be monitored, inspected, accessed, or examined by the School or by a third party on behalf of the School at any time without notification, for the following purposes:

- Facilitating the efficient operation and management of Ascham's ICT resources;
- Protecting the integrity of ICT resources;
- Investigating alleged misuse;
- Managing Ascham's copywrite obligations, e.g. anti-plagiarism software may be used.
- Auditing Ascham's assets; or
- Managing information security related activities.

Systems that monitor and filter use of the internet, both during School or working hours and outside of those hours, are in place at Ascham. This can include the sites and content that students and staff member's visit and the length of time they spend using these sites and services. Network access and internet traffic may also be monitored on School owned devices, both onsite and offsite, as well as BYOD devices (owned by either staff or students) when connected to the campus networks.

Usage of ICT systems licensed by Ascham, for example Microsoft 365 services may also be monitored regardless of whether they are accessed on School or personally owned devices.

Where considered appropriate, the School may block access to particular websites or email, both in coming and / or outgoing.

For cyber security purposes, geo-location access restrictions are enabled for certain systems. For example, access to Microsoft 365 from outside of Australia needs to be approved by exception.

6.8. Use of Generative AI

Ascham recognises that the integration of Generative (Gen) Artificial Intelligence (AI) into education can enhance teaching and learning experiences, but it must be done responsibly, ethically, and in alignment with our School values. Ascham aims to promote the efficient and ethical use of AI tools, while minimizing the risk of intentional or unintentional misuse that may result in harm to students, staff, the School itself, or the wider Ascham community. For more detail on the use of AI at Ascham, please refer to the Generative Artificial Intelligence Usage Policy.

6.9. Limited Personal Use

Authorised users may use Ascham internet and email facilities to send and receive personal messages, provided such use is kept to a minimum and does not interfere with their studies or performance of work duties.

- It should be noted that any use of the School network, internet or email for personal purposes is subject to the same terms and conditions as otherwise described in this policy.
- Excessive or inappropriate use of email or internet facilities for personal reasons by staff during working hours may lead to disciplinary action.

- When using ICT or electronic communication outside of work or School business, conduct will not be tolerated where it is likely to cause damage to the relationship between Ascham and the Authorised user or has the potential to damage the School's interests, good name, or reputation.

7. RELEVANT LEGISLATION

Copyright Act 1968 (Commonwealth)

Crimes Act 1900 (NSW)

Cybercrime Act 2001 (Commonwealth)

Defamation Act, 2005 (NSW)

Government Information (Public Access) Act, 2009 (NSW)

Privacy Act, 1998 (Commonwealth)

Privacy & Personal Information Protection Act, 1998 (NSW)

Spam Act 2003 (Commonwealth)

Workplace Surveillance Act 2005

8. KEY RELATED DOCUMENTS

Ascham Code of Conduct

Ascham Anti-Bullying Policy

Ascham Privacy Policy

Ascham Data Governance Policy

Ascham Information Security Policy

Ascham Generative Artificial Intelligence Policy

9. POLICY INFORMATION

Policy Number	AS02
Version	12
Policy Owner	Director of Information and Communication Technology
Authorised By	Head of School
Review Date	2025 | Term 1
Next Review Date	2026 | Term 1

Annex 1 – Staff Acceptable Use Guidelines

The following considerations and guidelines must be observed by staff when using Ascham ICT resources.

1. SECURITY

- All staff, including casual staff will be issued with unique logins to access Ascham ICT resources. Generic logins will not be issued unless there are exceptional circumstances. The Director of ICT must approve such circumstances.
- It is the responsibility of staff to ensure that their passphrase is kept secure; if staff are concerned that their passphrase has been compromised, they should change it immediately and notify Ascham IT.
- Staff are responsible for the physical security of all Ascham owned ICT hardware they are issued with. They must also safeguard any personal hardware used to access School ICT Services e.g., School email on a personal smart phone and let Ascham IT know immediately if the device is lost (so the email or other Ascham account can be secured).
- Personal devices accessing School ICT resources must have appropriate access protection activated e.g., password/passphrase, pin code, fingerprint, or facial recognition etc.
- When away from their desk, staff are required to lock device devices connected to the Ascham network to prevent unauthorised access. Devices must not be left unlocked at any time. Locking classroom or office doors is not a sufficient method of ensuring the security of the School's information.
- Remote access to the School's network is restricted to Ascham staff. Staff must only use School owned devices (or ICT approved BYO devices) with the Global Protect VPN to access the network remotely. When finished, sessions should be disconnected to ensure no unauthorized access is gained.
- Staff must comply with access requirements where multi-factor authentication is implemented for Ascham systems.
- Staff should only grant guest WiFi access to verified guests (when you receive a Clearpass email request to allow visitor WiFi access).
- ID cards are issued to staff provide access to photocopiers, boom gates and buildings so it is critical that staff inform Ascham IT immediately in the event that a card is lost so that it can be cancelled and reissued.
- All visitors to the School are required to sign in at Wallis or Hillingdon Reception areas so that the School has an accurate record of who is on campus at all times. Please direct your visitors to the reception areas to ensure they sign in.

2. EMAIL AND ONLINE MESSAGING CONTENT

- Email and online messaging correspondence should be treated in the same way as any other correspondence such as a letter.
- Email and Teams messaging are neither private nor secret; they can be easily copied, forwarded, saved, intercepted, or archived. The resulting audience of an inappropriate email may be unexpected and widespread.
- All email and Teams messaging are backed up by the School and may be requested / presented in litigation proceedings. This also applies to deleted items, which when you delete are only removed from your inbox account, not the Schools records.
- If a member of staff receives inappropriate material by email or Teams messaging, they should notify the Director of ICT. It should not be forwarded to anyone else. If possible, the staff member should discourage the sender, if known, from sending further material of that nature.
- When staff members communicate with current students via email or online messaging, the communication must always only be sent and received via the School provided email addresses or Teams messaging.
- Comments that are not appropriate in the workplace or school environment are also inappropriate when sent by email. Written messages may be misconstrued, accordingly, words and attached / linked documents should be carefully expressed in a clear, professional manner.

3. PRIVACY

- When using Ascham's ICT services in either a professional or personal capacity, staff must respect the privacy of the Ascham community at all times. Personally identifying information including (but not limited to) names, usernames, addresses, phone numbers, email addresses, photos and videos must not be disclosed without permission.
- When using online networking websites in either a personal or professional capacity, staff must:
    - Maintain professional standards.
    - Not accept current students or ex-students within 12 months of leaving the School, as "friends" on personal social networking sites. Staff must decline any friend requests initiated by students or former students who have left the School within the previous 12 months, or if the students or ex-students remain under age (less than 18 years of age).
    - Not initiate contact with current students or ex-students on online networking websites.
    - Not discuss students or colleagues online, nor publicly criticise School policies or personnel.
    - Not use any email address to set up social networking or internet accounts which identify Ascham, without prior approval from the Head of School.

- Be mindful at all times when using personal social media that people classified as "friends" have the ability to download and share information with others on many social networking sites.

4. SOCIAL NETWORKING SITES

When using Social networking sites such as, but not limited to, Twitter, Facebook, Instagram, Snapchat, Tik Tok and other web applications. Staff must:

- Ensure that use of social networking sites does not jeopardise the reputation of Ascham and its community, or the relationship of mutual trust and confidence between staff and the School.
- Be aware that certain conduct, even whilst outside the workplace and the School setting, may have a serious impact on the employment relationship with Ascham, to the extent that it could breach the employment contract between a member of staff and the School. Social networking applications and many of their postings cannot be controlled or removed and often have wide public exposure which neither staff nor Ascham can control once published. Any comments on social networking or other public sites found to be in breach of this policy may be cause for disciplinary action including termination of employment.
- Understand the serious risks when communicating with students on social networking sites. Staff members risk exposing themselves to allegations of inappropriate relationships with students, and to the responsibility of having to contend with any rule breaking or risky behaviour that may be observed through postings and images on students' pages.
- In a private capacity, use of these web sites must not negatively impact on the reputation of staff members of Ascham and must be sensitive toward the values and ethos of the School.
- Consider the adoption of high security settings on social networking sites to protect personal information. For example, staff should not make their content universally available, but should restrict access only to users they have approved. It is important to note even with high security settings, there is always a risk associated with uploading any personal information to the internet.

4.1. Educational Uses of Social Networking Sites

If staff members use social networking websites as a part of the educational process, they must:

- Use only restricted, Ascham approved networking websites, first seeking approval from their Head of Department and the Director ICT. When seeking approval, ensure that all aspects of the social networking website are available for assessment.
- Request that a Privacy Impact Assessment (PIA), against the Office of the Australian Information Commissioner's, Australian Privacy Principles (APP's) is conducted when wanting to use new online services.
- Comply with all instructions regarding maintaining the security of the School's ICT resources. This includes:

    - Consulting the Director ICT about the appropriateness of installing any external applications associated with a social networking site.
    - Running updated malware protection to avoid infections of spyware and adware that social networking sites might place on an Ascham computer.
- Communicate in ways that are professional, age-appropriate, and consistent with the Ascham values.
- Ensure that postings comply with relevant laws including, but not limited to, child protection, anti-discrimination, and copyright legislation.

See also the Ascham Data Governance, Information Security and Generative AI Policies for considerations when using external websites and hosted services.

Annex 2 - Ascham ICT Acceptable Use Guidelines – Hillingdon (Prep to Year 2)

All Ascham students, regardless of their age, use the School's Information and Communication Technology (ICT) resources as a part of their studies. To facilitate this, parents are required to accept the ICT Acceptable Use Policy (ICT AUP) on their daughter's behalf.

Acceptance of the ICT AUP confirms that you have read the policy and the guidelines below and discussed these with your daughter. You are confirming on her behalf that following that discussion she understands and will comply with the School's expectations of how students may use the School's ICT resources.

For parents, the ICT AUP should be read in conjunction with the following Ascham policies and code:

- Anti-Bullying Policy
- Ascham Privacy Policy
- Code of Conduct

The following Acceptable Use Guidelines outline the behaviours expected of your daughter when using Ascham ICT resources. These guidelines will be reviewed annually and if the School substantially amends this agreement, we will notify you of relevant changes.

ACCEPTABLE USE GUIDELINES FOR HILLINGDON STUDENTS

Digital Devices

Digital devices and internet services are provided by the School for students in Prep through to Year 2 to enhance their education. These digital devices and services must be used in a responsible manner. When using Ascham ICT Resources, students should know and understand:

- Technology is only to be used when permission is given, and a teacher is present.
- The settings on devices must not be altered.
- Devices are to remain in their protective cases.
- Devices are to remain in the classroom at recess and lunch.
- Proper care must be taken when using or carrying devices.
- Any damage should be reported to the teacher.
- Devices should be stored correctly.
- Devices must only be used for the purpose of the set learning activity.

Cyber Safety

With regard to cyber-safety and cyberbullying, students should know and understand:

- Passwords/passphrases must be kept private.

- Personal information including full names, addresses, phone numbers, email addresses and photos of themselves, friends or family must be kept private.
- Students should not be mean, rude, or unkind to, or about other people when using devices.
- If they see anything that is upsetting, mean or rude they will not show others, they will turn off or close the screen and notify a teacher straight away.
- Photographs or videos must not be taken of other students or staff members without teacher permission during learning activities.
- Students should only access websites that teachers have selected and are relevant to their studies and should make no attempt to access other, particularly inappropriate material.
- Disabling browsing history on School owned devices is not permitted, and teachers may access students' browsing history from time to time.

At Home

With technology increasingly becoming part of students' everyday lives and students having greater access to technology at a younger age, the School makes the following recommendations about technology use at home:

- Parents should monitor the amount of screen time their children have.
- Technology is kept out of bedrooms (this includes gaming devices, televisions, iPads, phones and laptops).
- It is used under the supervision and guidance of an adult.
- Parents set the proper parental controls on student devices and manage accessibility to age-appropriate content via the internet, App and Google Play stores.
- Devices should not used one hour prior to bedtime, or before sleeping because of the negative effects of blue light on sleeping patterns.

Internet and Social Media Use

At Ascham we believe social media can be an important way for students to connect with each other and the world. However, the School day is not an appropriate time to use social media and no student should use it during School hours. It should be understood that a student is always a member of the Ascham Community and if using social media outside of School hours, students must abide by Ascham's policies at all times.

When using social media, students should understand the importance of making good choices such as ensuring strong privacy settings, using appropriate language and behaviour, and ensuring their own and others' safety at all times. They can do this by following the Acceptable Use Guidelines listed below.

- Social media accounts such as Facebook, Instagram, SnapChat and Tik Tok etc are not permitted under the age of 13 and are therefore not appropriate for Hillingdon students. Parents must always check for age restrictions before setting up any social media account or downloading an app.

- Students should only use their School account to access the internet; the use of devices with mobile data is not permitted at School.
- Students should access websites that are relevant to the information that they need for their studies and should make no attempt to access inappropriate material.
- Students may not use internet chat, personal email (e.g., Gmail or Hotmail), social networking sites and instant messaging services during the School day.
- When using the Ascham network, students may not download or install any films, TV series, music or games from the internet.
- Students should respect the privacy of everyone and should not post any inappropriate comments or images of the Ascham Community or third-party contractors.
- Students (and parents) may not publish photographs or videos containing students in Ascham uniform (including sport uniform) or on School grounds, including geo-location tagging, on a public forum or shared in any other public forum without the express consent of the School. To do so is a breach of privacy and the Schools Social Media policy.
- Social media when used inappropriately can lead to cyberbullying, harassment and unlawful behaviour. It is important that all Students follow the above protocols to ensure the safety and wellbeing of each other when engaging on social media.

Mobile Phones

- Mobile phones or other devices such as smartwatches (with cellular access) may not be used or accessed during School hours.
- Students in Years Prep to 2 are not permitted to bring mobile phones to School.
- Any girl who brings a smartwatch (with cellular access) to School must hand it in to their class teacher first thing in the morning and be responsible for collecting it as they leave in the afternoon.
- Girls found with a mobile phone or a smartwatch (with cellular access) during the School day will have it confiscated.

Copyright

Ascham students are taught that copying another person's work, without acknowledgement is plagiarism and constitutes infringement of the Copyright Laws. Infringing Copyright laws may include illegally copying, distributing, or sharing software, images, video, music or other published works without permission from the original owner. Ascham may use anti-plagiarism software to assist in maintaining its licensing and copywrite obligations.

General Protocols

- Students should respect the privacy of all members of the School community. The reputation of each student, teacher, parent, community member and of the School itself is important and should never be caused harm.

- Students should not post any comment or image that is hurtful, embarrassing, or unkind. They should only post comments and images about their friends that they would be prepared to have made public. Students should not post any comments or images about the School or any member of staff.
- Students should maintain the highest security in their privacy settings on all social media and should not have any private information publicly visible.
- Blogs, tweets, and other forms of commentary on the internet should not say anything that is misleading, malicious or untrue. Unkind and hurtful comments should never be made about any member of the School community.
- Students should not impersonate or falsely represent another person.
- It is strongly recommended that, on social networking sites, students only accept friends and followers that they know well enough to speak to. No student is allowed to request a member of staff to be a social media 'friend'.

Consequences

If a student does not follow the School's protocols with regard to ICT and social media use, the consequences may include:

- Any form of deliberate cyber bullying, harassment or unlawful behaviour will be reported immediately to the Head of Junior School and may lead to more serious consequences.
- Parents will be informed of any social media misconduct by the student.
- All reports of Cyber bullying and other technology misuses will be investigated fully and may result in a notification to police where the School is obligated to do so. Students and parents must be aware that in certain circumstances where a crime may have been committed, they may be subject to a criminal investigation by Police over which the School have no control.

Annex 3 - Ascham ICT Acceptable Use Guidelines – Fiona & Senior School (Year 3 to Year 12)

All Ascham students, regardless of their age, use the School's Information and Communication Technology (ICT) resources as a part of their studies. From Year 3, students are issued with individual account access to the School's network and are required to accept the ICT Acceptable Use Policy (ICT AUP), in addition to their parents' acceptance on their behalf.

Acceptance of the form confirms that you and your daughter have read the ICT AUP and the guidelines below, and that she understands and will comply with the School's expectations of how students may use the School's ICT resources.

For parents, the ICT AUP should be read in conjunction with the following Ascham policies and code:

- Anti-Bullying Policy
- Ascham Privacy Policy
- Code of Conduct

The following Acceptable Use Guidelines outline the behaviours expected of your daughter when using Ascham ICT resources. These guidelines will be reviewed annually and if the School substantially amends this agreement, we will notify you of any relevant changes.

ACCEPTABLE USE GUIDELINES FOR FIONA & SENIOR SCHOOL

Network use

- Students should log on to the School's network with the username and passphrase the School has issued them, and not share this information with other students.
- If students are concerned about the privacy of their passphrase, they should visit the IT Help Desk so that it can be changed.
- When using School owned computers, it is important to log off at the end of each session to avoid unauthorised activity.
- Students must not compromise network security by attempting to bypass or corrupt any hardware and / or software protection.
- Students must not use a virtual private network or VPN software either directly installed on their laptop or via web browser extensions whilst on School networks. This includes using VPN software to mask internet browsing, bypass School protections or network filtering.
- Students should use their Microsoft 365 OneDrive to store their work as these drives are backed up every day. USB drives may be useful for transporting files but are not recommended for permanent storage.

- Microsoft 365 OneDrive is only to be used to store School related data i.e., no personal files including photos, videos, or non-School related programs. These files may be deleted.
- Students should minimise printing by print previewing, editing and spell checking on screen.
- Students should report any problems they experience with classroom devices to their teacher.
- The IT Department monitors student access to the network (including file storage, email and internet usage) without any notification. Inappropriate use of the network may result in the withdrawal of access to ICT facilities within the School.

BYOD - Personal Devices (Year 5 to Year 12)

- School data on student personal devices should be regularly backed up to either the student's cloud storage via Microsoft Office 365 OneDrive or (for certain Art students) the network devices provided by the School. Please contact the IT Department if you require assistance or further information.
- All student laptops connecting to the School's network must be safeguarded with up-to-date antivirus and anti-malware software. We recommend and provide Microsoft Defender Advanced Threat Protection for both Windows and Mac operating systems at no cost and this can be installed by the Ascham IT Help Desk. If parents opt for an alternative solution, it is their responsibility to ensure it remains current. Devices without adequate protection may face restricted access or be blocked from the network and Ascham resources.
- It is recommended that a protective case be used with student laptops to avoid damage.
- The School is not responsible for damage or faults with personally owned devices; it is recommended that parents consider insurance against theft and accidental damage.
- Students are not permitted to play games/music/videos in class.
- Students must ask their teachers for permission to use their headphones during Studies.
- Inappropriate use of personal devices may lead to a detention.
- Continued inappropriate use may lead to the student having her School internet access denied for a period of time and further education of appropriate use to occur.

Internet and Social Media Use

At Ascham we believe social media can be an important way for students to connect with each other and the world. However, the School day is not an appropriate time to use social media and no student should use it during School hours. It should be understood that a student is always a member of the Ascham Community and if using social media outside of School hours, students must abide by Ascham's policies at all times.

When using social media, students should understand the importance of making good choices such as ensuring strong privacy settings, using appropriate language and behaviour, and ensuring their own and others' safety at all times. They can do this by following the Acceptable Use Guidelines listed below.

- Social media accounts such as Facebook, Instagram, SnapChat and Tik Tok are not permitted under the age of 13 and are therefore not appropriate for Fiona students. Parents must always check for age restrictions before setting up any social media account or downloading an app.
- Students should only use their School account to access the internet; the use of devices with mobile data is not permitted at School.
- Students should access websites that are relevant to the information that they need for their studies and should make no attempt to access inappropriate material.
- Students may not use internet chat, personal email (e.g., Gmail or Hotmail), social networking sites and instant messaging services during the School day.
- When using the Ascham network, students may not download or install any films, TV series, music, or games from the internet.
- Students may not publish any comments regarding Ascham, Ascham staff, Ascham students or other students on the internet and/or any social networking sites; this can be classified as cyberbullying.
- Students must not impersonate another person by signing them up to websites or services without their knowledge or consent.
- Students must not make video or audio recordings of staff or other students without their knowledge or consent.
- Students (and parents) may not publish photographs or videos containing students in Ascham uniform (including sport uniform) or on School grounds, including geo-location tagging, on a public forum or shared in any other public forum without the express consent of the School. To do so is a breach of privacy and the Schools Social Media policy. This includes any social networking sites such as Facebook, YouTube, Instagram, Snapchat TikTok etc.
- Students may not publish any images of the Ascham School site itself.
- Students must not share outside of the School any Ascham recorded lessons (either audio or video) or written material from Ascham lessons. The only exception is where either directed or approved by an Ascham staff member.
- Students must understand the importance of using social media responsibly and keeping within the Law. Social media when used inappropriately can lead to cyber-bullying, damage to reputation, harassment, and unlawful behaviour. It is important that all Students follow the above protocols to ensure the safety and wellbeing of each other when engaging on social media.

Email and Online Messaging Use

- Ascham provided email and online messaging accounts (e.g., Microsoft Teams) are to be used for School related purposes only.
- Students may not use non-School email accounts such as Hotmail and Gmail etc when at School.
- Email messages must be polite and upper case by itself should not be used.
- Students may not send email messages that harass or bully.
- It is recommended that Students proof-read and edit emails before sending.
- Email messages should be composed using full words not abbreviations (e.g., ‘thanks’ not ‘thx’).

- Students may not send any attachments greater than 10MB.
- Students should delete any unnecessary emails.
- Students must respect copyright procedures.
- Students should contact the Ascham IT or a staff member immediately if an email is received that causes concern.
- Inappropriate use of email may result in the withdrawal of access to ICT facilities within the School.

Mobile Phones

- Mobile phones or other devices such as smartwatches (with cellular access) may not be used or accessed during School hours.
- Fiona students (Years 3 to 6) who travel on public transport or walk to or from School are permitted to bring mobile phones to School. They must hand them to their Class Teacher first thing in the morning and be responsible for collecting them as they leave in the afternoon.
- Senior School students (Years 7 to 12) must hand in their phone to their Form Teacher each morning and be responsible for collecting them as they leave in the afternoon.
- Students found with a mobile phone or a smartwatch (with cellular access) during the School day will have it confiscated.

Copyright

Ascham students understand that copying another person's work, without acknowledgement is plagiarism and constitutes an infringement of the Copyright Laws. Students must correctly reference direct quotations, facts and figures, as well as ideas and theories, from all sources that are not their own work, including AI sources. Infringing Copyright laws may include illegally copying, distributing or sharing software, images, video, music or other published works without permission from the original owner. Ascham may use anti-plagiarism software to assist in maintaining its licensing and copywrite obligations.

General Protocols

- Students must not disclose their passphrase to anyone.
- Students should respect the privacy of all members of the School community. The reputation of each student, teacher, parent, community member and of the School itself is important and should never be caused harm.
- Students should not post any comment or image that is hurtful, embarrassing, or unkind. They should only post comments and images about their friends that they would be prepared to have made public. Students should not post any comments or images about the School or any member of staff.
- Students should maintain the highest security in their privacy settings on all social media and should not have any private information publicly visible.

- Blogs, tweets, and other forms of commentary on the internet should not say anything that is misleading, malicious, or untrue. Unkind and hurtful comments should never be made about any member of the School community.
- Students should not impersonate or falsely represent another person.
- Once a girl reaches 13, the School can assist her, with parents' permission, in setting secure privacy settings for age restricted social media and with guidance in appropriate social media behaviour.
- It is strongly recommended that, on social networking sites, students only accept friends and followers that they know well enough to speak to. No student is allowed to request a member of staff to be a social media 'friend'.

Consequences

If a student does not follow the school's protocols with regard to social media use, the consequences may include:

- A student who does not follow the protocols due to lack of knowledge will be required to have a compulsory education session on privacy settings and appropriate social media behaviour.
- Any form of deliberate cyber bullying, harassment or unlawful behaviour on social media will be reported immediately to the Head of School / Head of Junior School and may lead to more serious consequences.
- Parents will be informed of any social media misconduct by the student.
- A Senior School student who misuses social media will be put on Saturday Detention and/or be asked to fulfil a required number of hours of School community service (such as cleaning chewing gum, litter collection, tidying up the gym etc.).
- All reports of cyber bullying and other technology misuses will be investigated fully and may result in a notification to police where the School is obligated to do so. Students and Parents must be aware that in certain circumstances where a crime may have been committed, they may be subject to a criminal investigation by Police over which the School will have no control.