ALDENHAM
SCHOOL

Acceptable Use of ICT and Mobile Devices Policy for Students

January 2026
by Head of Technology (JC)

Scope

This policy applies to all students at Aldenham School who use school IT systems as a condition of access. The School provides a computing network which allows a range of devices to connect. The policy sets out the way in which devices should be used and includes guidelines for the safe and responsible use of the network and the internet and identifies those activities which constitute an abuse of our ICT facilities.

Parents are encouraged to read this policy with their child. The School actively promotes the participation of parents to help the School safeguard the welfare of pupils and promote the safe use of technology.

Aims

The aims of this policy are as follows:

- To educate and encourage pupils to make good use of the educational opportunities presented by access to technology.
- To safeguard and promote the welfare of pupils, in particular by anticipating and preventing the risks arising from:
    - exposure to harmful or inappropriate material (such as pornographic, racist, extremist or offensive materials).
    - the sharing of personal data, including images.
    - inappropriate online contact or conduct.
    - cyberbullying and other forms of abuse.
- To minimise the risk of harm to the assets and reputation of the School.
- To help pupils take responsibility for their own safe use of technology.
- To ensure that pupils use technology safely and securely and are aware of both external and peer-to-peer risks when using technology.
- To prevent the unnecessary criminalisation of pupils.

School Policies

The following School policies, procedures and resource materials are relevant to this policy:

- Behaviour Policy.
- Anti-Bullying Policy.
- Online Safety Policy.
- Safeguarding Policy.

The School will take a wide and purposive approach to considering what falls within the meaning of technology. This policy relates to all technology, computing and communications devices, network hardware and software, and services and applications associated with them including:

- The internet
- Email
- Mobile phones and smartphones
- Desktops, laptops, netbooks, tablets
- Personal music players
- Devices with the capability for recording and / or storing still or moving images
- Social networking, micro blogging and other interactive websites

- Instant messaging (including image and video messaging via apps such as Snapchat and WhatsApp), chat rooms, blogs and message boards.
- Webcams, video hosting sites (such as YouTube)
- Gaming sites
- Virtual learning environments
- Interactive Screens
- Other photographic or electronic equipment e.g. GoPro devices.

Safe use of technology

We want pupils to enjoy using technology and to become skilled users of online resources and media. We recognise that this is crucial for further education and careers.

The School will support pupils to develop their skills and make internet access as unrestricted as possible whilst balancing the safety and welfare of pupils and the security of our systems. The safe use of technology is integral to the School's curriculum. Pupils are educated about the importance of safe and responsible use of technology to help them to protect themselves and others online.

Pupils may find the following resources helpful in keeping themselves safe online:

- http://www.thinkuknow.co.uk/
- http://www.childnet.com/young-people
- https://www.saferinternet.org.uk/advice-centre/young-people
- https://www.disrespectnobody.co.uk/
- http://www.safetynetkids.org.uk/
- http://www.childline.org.uk/Pages/Home.aspx

Please see the School's Online Safety Policy for further information about the school's online safety strategy.

I**nternet and email**

All pupils will receive guidance on the use of the school's internet and, where accessible, email systems. If a pupil is unsure about whether they are doing the right thing, they must seek assistance from a member of staff.

For the protection of all pupils, their use of email and of the internet will be monitored by the school. Pupils should remember that even when an email or something that has been downloaded has been deleted, it can still be traced on the system. Pupils should not assume that files stored on servers or storage media are always private.

School Rules

Pupils **must** comply with the following rules and principles:

- Access and security (Appendix 1)
- Use of internet, email and other online communication (Appendix 2)
- Use of mobile electronic devices (Appendix 3)
- Photographs and images (including "sexting") (Appendix 4)

The purpose of these rules is to set out the principles which pupils must bear in mind at all times and also the rules which pupils must follow to use technology safely and securely.

These principles and rules apply to all use of technology.

Procedures

Pupils are always responsible for their actions, conduct and behaviour when using technology. Use of technology should be safe, responsible and respectful to others and the law. If a pupil is aware of misuse by other pupils, they should talk to a teacher about it as soon as possible.

Any misuse of technology by pupils will be dealt with under the School's Behaviour Policy. Incidents involving the misuse of technology which are of a safeguarding nature will be dealt with in accordance with the School's Safeguarding Policy in conjunction with the School's Behaviour Policy. If a pupil is worried about something that they have seen on the internet, or on any electronic device, including on another person's electronic device, they must tell a teacher about it as soon as possible.

Pupils must not use their own or the school's technology to bully others. Bullying incidents involving the use of technology will be dealt with under the School's Anti-Bullying Policy. If a pupil thinks that they might have been bullied or that another person is being bullied, they should talk to a teacher about it as soon as possible. See the School's Anti-Bullying Policy for further information about cyberbullying and e-safety, including useful resources.

In a case where the pupil is potentially vulnerable to radicalisation, they may be referred to the Channel programme in accordance with the School's Safeguarding Policy. Channel is a programme which focuses on support at an early stage to people who are identified as being vulnerable to being drawn into extremism (including terrorism).

Sanctions

Where a pupil breaches any of the school's rules, practices or procedures set out in this policy or the appendices, the respective Head will apply any sanction which is appropriate and proportionate to the breach in accordance with the School's Behaviour Policy including, in the most serious cases, permanent exclusion.

Unacceptable use of technology could lead to the confiscation of a device or deletion of the material in accordance with the procedures in this policy.

If there are reasonable grounds to suspect that the confiscated device contains evidence in relation to an offence e.g. upskirting, or that it contains a pornographic image of a child or an extreme pornographic image, the device will be given to the police. See Appendix 4 for more information on photographs and images.

The school reserves the right to charge a pupil or their parents for any costs incurred to the School because of a breach of this policy.

Record keeping

All records created in accordance with this policy are managed in accordance with the law and the school's policies that apply to the retention and destruction of records.

The records created in accordance with this policy may contain personal data. The school has Privacy Notices which explain how the school will use personal data about pupils and parents. The Privacy Notices are published on the school's website. In addition, staff must ensure that they follow the School's Data Protection Policy when handling personal data created in

connection with this policy. Information Security and Sharing Data guidance is also contained in the Data Protection Policy.

The computer system is owned by The Aldenham Foundation and the Foundation reserves the right to examine or delete any files, including email, that may be held on its computer system or to monitor any Internet sites visited. Aldenham School reserves the right to vary the terms of this agreement/policy at any time and without prior notice. Aldenham Foundation has the right to withdraw access to the Network, suspend Internet access or email access. Network access will be suspended until any policy discrepancy has been finalised. The decision of Aldenham Foundation is final. The latest Agreement is always available for download from the home page of My School Portal or by contacting the School. It is important that you review the Agreement regularly to ensure you are aware of any changes.

Appendix 1

Access and Security

1. Access to the internet from the school's computers and network must be for educational purposes only.

2. You must not knowingly obtain (or attempt to obtain) unauthorised access to any part of the school's or any other computer system, or any information contained on such a system.

3. Use of any pupil laptop or other mobile electronic device connected to the School's Wi-Fi is also covered by this policy regarding acceptable behaviour.

4. Pupils accessing the internet outside the school's network whilst on School premises or otherwise in the care of the School do so at their own risk and must comply with all the provisions of this policy regarding acceptable behaviour. If a pupil's device can access the internet outside of the school Wi-Fi network, then parents must ensure that appropriate security and filtering is enabled on their child's device.

5. Passwords protect the school's network and computer system. You must not let anyone else know your password. If you believe that someone knows your password, you must change it immediately.

6. You must not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you are not authorised to access. If there is a problem with your passwords, you should speak to your class teacher or contact the Head of Technology.

7. You must not attempt to access or share information about others without the permission of the Head of Technology. To do so may breach data protection legislation and laws relating to confidentiality.

8. The school has a firewall in place to ensure the safety and security of the school's networks. You must not attempt to disable, defeat or circumvent any of the school's security facilities. Any problems with the firewall must be reported to the class teacher or the Head of Technology.

9. The school has filtering systems in place to block access to unsuitable material, wherever possible, to protect the welfare and safety of pupils. You must not try to bypass this filter.

10. Viruses can cause serious harm to the security of the school's network and that of others. Viruses are often spread through internet downloads or circulated as attachments to emails. If you think or suspect that an attachment, or other downloadable material, might contain a virus, you must speak to a member of the IT team before opening the attachment or downloading the material.

11. You must not disable or uninstall any anti-virus software on the school's computers.

12. The use of location services represents a risk to the personal safety of pupils and to School security. The use of any website or application, whether on a School or personal device, with the capability of identifying the user's location while you are on School premises or otherwise in the care of the school is discouraged.

Appendix 2

Use of the Internet and Email

1. The school does not undertake to provide continuous internet access. Email and website addresses at the school may change from time to time.

Use of the Internet

2. You must take care to protect personal and confidential information about yourself and others when using the internet, even if information is obtained inadvertently. You should not put personal information about yourself, for example your full name, address, date of birth or mobile number, online.

3. You should assume that all material on the internet is protected by copyright and such material must be treated appropriately and in accordance with the owner's rights - you must not copy (plagiarise) another's work.

4. You must not view, retrieve, download, or share any offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory, or criminal activity. Use of technology in this way is a serious breach of discipline and may constitute a serious criminal offence. You must tell a member of staff immediately if you have accidentally read, downloaded or have been sent any offensive material or material that is inappropriate, including personal information about someone else.

5. You must not communicate with staff using social networking sites or other internet or web-based communication channels.

6. You must not bring the school into disrepute through your use of the internet.

Use of Email

7. You must use your school email accounts for any email communication with staff. Communication either from a personal email account or to a member of staff's personal email account is not permitted.

8. Email should be treated in the same way as any other form of written communication. You should not include or ask to receive anything in an email which is not appropriate to be published generally or which you believe the school and / or your parents would consider to be inappropriate. Remember that emails could be forwarded to or seen by someone you did not intend.

9. You must not send or search for any email message which contains offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory, or criminal activity. If you are unsure about the content of a message, you must speak to a member of staff. If you come across such material, you must inform a member of staff as soon as possible. Use of the email system in this way is a serious breach of discipline and may constitute a criminal offence.

10. Trivial messages and jokes should not be sent or forwarded through the school's email system. Not only could these cause distress to recipients (if considered to be inappropriate) but could also cause the school's network to suffer delays and / or damage.

11. All correspondence from your school email account must contain the School's disclaimer.

12. You must not read anyone else's emails without their consent.

Other Online Communication (including social media)

13. Anything you post online whether through messaging, social media or by other means needs to be considered carefully. Remember that there is a 'disinhibition effect' making you more likely to post things you might regret. The school may become involved in anything between members of the school community or that may bring the school into disrepute. Private conversations are rarely private and should not be considered so.

14. Only post messages or images you would be happy for a teacher, parent, or guardian to see. Avoid making strongly opinionated comments which could be deemed offensive. Avoid making comments related to protected characteristics.

15. Anonymous posting is unwise. If pupils set up accounts to post anonymously (or that the presence of a group allows anonymity) all members of the group will be deemed individually responsible for material posted unless an individual admits responsibility. Nevertheless, other members of the group will be deemed partially responsible unless they have reported inappropriate posts or actively attempted to dissuade the perpetrator.

16. Do not make comments about individuals or the school online. They may be your views, but they could cause offence and the internet is not the place for such comments.

17. Never pose as anyone else or any institution.

18. Do not harass others or post things intended to upset them. Do not troll.

19. Some messages and images may seem to be temporary and permanently deleted – this may not be the case if screenshots or photos are taken. Treat all posts as permanent.

20. Be cautious of meeting someone you meet online in real life. Always take an adult with you and tell people where you are going and who you are meeting.

21. Remember: once you share something it can be freely and easily copied, shared, or manipulated. Once you have shared it – you have lost control of it.

22. Do not use ICT in your bedroom as it affects sleep and can make it more likely that you will post something you will regret. It is also best to avoid using ICT when tired. Switch off an hour before bedtime and leave devices out of the bedroom.

23. Consider how much ICT you use in a day. Use of the internet and gaming can both be addictive. It is difficult to self-regulate use.

24. Be careful not to believe all you read online. Some sites publish dangerously inaccurate

material. Be especially careful when investigating health concerns, sexuality and identity and searching for supportive communities.

Appendix 3

Use of Artificial Intelligence (AI)

AI – artificial intelligence – any system that displays apparently intelligent behaviour by analysing the environment/inputs and taking actions to achieve specific goals. In education this can include assessing student progress, personalising learning, analysing data, supporting ideas generation etc.

This agreement covers all AI tools, including generative AI tools such as ChatGPT and DALL-E, whether stand-alone products or integrated into productivity suites, e.g., Co-Pilot in Microsoft 365. This policy relates to all content creation, including (but not limited to) text, artwork, graphics, video and audio.

Introduction

AI has great potential to support your learning over time. AI can provide prompts and ideas, support in consolidating your knowledge, provide ideas for improving your work. Overuse or inappropriate use of AI has the potential to damage your educational development. Dishonest use can lead to severe sanctions internally in the school, and with awarding bodies (examination boards).

Central to appropriate use of AI in your learning and assessment is understanding what AI can and cannot do, when you are and are not allowed to use of AI, and correctly acknowledging when AI has been used in your work.

AI tools such as ChatGPT (which is a Large Language Model or LLM) are useful in generating ideas and testing out your thinking. However, you should know that the material generated by these programs may be inaccurate, incomplete, or otherwise problematic. You should check and verify ideas and answers against reputable source materials (for example textbooks, encyclopedias, trusted websites etc). AI tools can present incorrect or fake information as fact, and present fake citations. Code generation models can produce inaccurate outputs. Image generation models can produce biased or offensive products.

AI can get you to answers quickly, without you having to go through the struggle of developing an understanding. A balanced use of AI is important in ensuring that you are actually learning and developing, rather than just giving the 'right answer'.

Appropriate Uses of AI in School (for Students)

If you are unsure on whether you may or may not use AI tools for a particular piece of work, communicate with your teacher. You are responsible for any content you submit, regardless of whether it originally comes from you or from an AI tool.

As general rule, you may use AI tools to help inform your everyday learning and school work. This may include in-class work, homeworks, activities etc. However, you must clearly indicate which tool(s) you have used to generate any content. In some learning situations you will be specifically asked to use AI tools to enhance your learning, and to explore and understand how these tools can be used.

For any learning and work that is being assessed (including in-class and prep/homework) and particularly when being assessed for external qualifications (GCSEs, A Levels, EPQ) etc:

- Your teacher will give you explicit instructions on whether AI tools can be used
- If AI tools are permitted, how these tools can be used.

In some circumstances use of AI tools will be forbidden, and use of these tools may be considered malpractice – see below. Some tasks may be created in a way such that AI tools cannot be used – eg working offline or under supervised conditions.

AI Misuse for Examinations

Our school abides by the JCQ AI Misuse Policy for examinations summarised below.

AI tools must only be used when the conditions of the assessment permit the use of

the internet and where the student is able to demonstrate that the final submission is

the product of their own independent work and independent thinking.

Examples of AI misuse include, but are not limited to, the following:

- Copying or paraphrasing sections of AI-generated content so that the work is no longer the student's own
- Copying or paraphrasing whole responses of AI-generated content
- Using AI to complete parts of the assessment so that the work does not reflect the student's own work, analysis, evaluation or calculations
- Failing to acknowledge use of AI tools when they have been used as a source of information
- Incomplete or poor acknowledgement of AI tools
- Submitting work with intentionally incomplete or misleading references or bibliographies

Consequences for misconduct in the use of AI

Where the school judges that AI tools have been used inappropriately, consequences may include:

- Any plagiarism or other forms of cheating will be dealt with under existing school policies.
- Your privileges in using AI tools may be curtailed, even when allowed in your learning / coursework etc.

Work being produced for 'Non-Examined Assessments (NEAs)' requires separate additional signed authentication by you, the student/candidate. Any suspected misuse of AI tools in NEA work with accompanying signed authentication will be reported to the relevant awarding body (examination board).

Appendix 4

Mobile Phone and Code of Use

1. Phones are not to be used during school. Every student from Years 7-11 has been assigned a personal Yondr Pouch. It is each student's responsibility to bring their Pouch with them to school every day and keep it in good working condition. Within boarding, students will be able to access their phones from the end of the school day. Students in Years 12 and 13 are not required to use a Pouch. They may only access their phones within the Sixth Form Centre or if instructed to by a member of staff. All of this information can be found in our Yondr phone policy.

2. It is always the responsibility of those bringing mobile phones to school to keep them in a safe place, either on the person or locked away. **The School does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto School premises, including devices that have been confiscated of which have been handed in to staff.**

3. Mobile phones are banned from any examination room even if switched off. **Contravention of this ban is likely to result in disqualification from the examination.**

Photographs and Images

1. Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

2. You may only use cameras or any mobile electronic device to take a still or moving image with the express permission of the member of staff in charge and with the permission of those appearing in the image.

3. You must allow staff access to images stored on mobile phones and / or cameras and must delete images if requested to do so. If the material found is a pornographic image of a child or an extreme pornographic image this will not be deleted and the device will be delivered to the police.

4. If material found on a device is a still or moving image that has been obtained by 'upskirting' this will not be deleted and the device will be delivered to the police.

5. The posting of images which in the reasonable opinion of the School are considered to be offensive or which brings the School into disrepute on any form of social media or websites, such as YouTube, is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material, irrespective of whether the image was posted using School or personal facilities.

Sexting

1. Sexting means the taking and sending or posting of images or videos of a sexual or indecent nature of you or another pupil, usually through mobile picture messages or webcams over the internet.

2. Sexting is strictly prohibited, whether you are in the care of the school at the time the image is recorded and / or shared, or not.

3. Sexting may be a criminal offence, even if the picture is taken and shared with the permission of the person in the image. Even if you are not prosecuted, this may result in information being

stored on your police record, which may prevent you from obtaining certain jobs in the future and may impact your freedom of travel.

4. The police may seize any devices which they believe may have been used for sexting. If the police find that a device contains inappropriate images, they are unlikely to return it to you.

5. Remember that once a photo or message is sent, you have no control about how it is passed on. You may delete the image, but it could have been saved or copied and may be shared by others.

6. Images shared online become public and may never be completely removed. They could be found in the future by anyone, even by universities and future employers.

7. Even if you do not share images yourself, there is a risk that you may lose your device, it may be "hacked", or its data may still be accessible to a future owner.

8. The school will treat incidences of sexting (both sending and receiving) as a breach of discipline and as a safeguarding matter under the School's child protection procedures (see the School's Safeguarding Policy). If you are concerned about any image you have received, sent, forwarded, or otherwise seen, speak to any member of staff for advice.

9. If sexual images or videos have been made and circulated online, you can be supported to get the images removed through the Internet Watch Foundation.

Upskirting

10. Upskirting typically involves taking a picture under a person's clothing without them knowing, with the intention of viewing parts of their body or clothing, not otherwise visible, to obtain sexual gratification, or cause the victim humiliation, distress, or alarm.

11. Upskirting is strictly prohibited, whether you are in the care of the School at the time the image is recorded, or not.

12. Upskirting is a criminal offence. Attempting to commit an act of upskirting may also be a criminal offence e.g. if actions are taken to do something that is more than merely preparatory to committing the offence such as attempting to take a photograph on a telephone or camera but failing to do so because of lack of storage space or battery.

13. The School will treat incidences of upskirting as a breach of discipline and as a safeguarding matter under the School's child protection procedures (see the School's Safeguarding Policy).

14. If you are concerned that you have been a victim of upskirting, speak to any member of staff for advice.

Appendix 5

Filtering, Monitoring and Online Safety

- Aldenham School is committed to providing a safe and secure digital environment for all pupils. To achieve this, we employ a robust, multi-layered approach to filtering and monitoring online activity. Our internet filtering is managed through Fortigate, a leading firewall solution that blocks access to inappropriate, harmful, or illegal content in line with statutory guidance and the school's safeguarding priorities. In addition, we use Securly for real-time monitoring of pupil activity across school devices and accounts, enabling proactive identification and intervention in cases of potential risk, misuse, or safeguarding concerns.

- Both systems are reviewed annually to ensure they remain effective and up to date with the latest threats and regulatory requirements. The school's leadership team, including the Designated Safeguarding Lead (DSL), oversees the effectiveness of these systems and ensures that all incidents are escalated and addressed appropriately. Our filtering and monitoring extend to emerging technologies, including generative AI tools, to ensure that risks associated with new forms of content are managed effectively.

- Pupils and parents are informed about the school's online safety measures and are encouraged to report any concerns. Regular training is provided to staff and students on safe and responsible use of technology, recognising online risks, and understanding the importance of digital wellbeing. The school's approach is guided by the latest Keeping Children Safe in Education (KCSIE) and Department for Education (DfE) guidance and is reviewed annually as part of our ongoing commitment to safeguarding and online safety.

ICT Acceptable Use Agreement for Pupils

I understand that use of the ICT resources at Aldenham School must be in support of educational research or learning and must not in any way bring the School's name into disrepute. I agree to the following:

- I will keep my password secure and will only use a network computer whilst logged on with my correct username and password.
- I will not share my username and password with anyone. I will always log off when leaving a workstation even for a short period.
- I will notify a member of staff immediately if I identify a security problem including SPAM or viruses.
- I will refrain from accessing any newsgroups, links, list-servers, Web Pages or other areas of cyberspace that would be considered as offensive by the School or my parents/guardians, because of pornographic, racist, violent, illegal, illicit, immoral or other content. I am responsible for rejecting these links if any appear inadvertently during my research. If such a website appears, I will report it to a member of staff.
- I will not use valuable Internet time playing non-educational games or using 'Chat' programmes. I will not download materials that may be copyrighted. I will not

violate copyright laws.

- I will not use, send or receive any material that could cause offence or harassment or is illegal.
- I will be courteous and use appropriate language in any e-mail I may send to other users. I understand that the laws of libel and copyright may apply to e-mail.
- I will not include any defamatory remarks about the School in any electronic communication including postings to any website. blogs, wiki's, msn, social utility sites (e.g. Facebook) and online streaming services (e.g. You Tube).
- I will not accept a friend request on Social Networking sites from anyone I do not know.
- "Plagiarism is unacceptable". I will use downloaded materials in an appropriate manner in assignments, listing them in a bibliography and clearly specifying directly quoted material. Failure to disclose sources may lead to exclusion from public exams.
- I will not reveal any personal information of any type about others or myself.
- I understand that the school web filter monitors all Internet activity.
- I will not store any executable data in my OneDrive, Teams or shared resource areas, without prior permission from a member of the ICT support staff.
- I will not store any files other than school related work; this includes all multimedia files i.e. videos and music.
- I will not attempt to physically connect any device directly to the School's network, this includes personal laptops, PlayStation, wireless access points, etc. (Webcams are also not permitted).
- I will not interfere with the set-up of software or hardware of any kind. If there is a problem with a system.
- I will not attempt to fix it myself but will inform the appropriate member of staff.
- I will not exploit the use of Skype or its services and understand it is a means of communication for pupils and their families only.
- I am aware of my social responsibilities with regard to using the internet and related technologies, including treating others with respect and reporting instances of online/cyber bullying.
- I understand that there may be occasions when I will access the internet without direct staff supervision e.g. when using computers out of hours or using the school's internet hotspots, but I agree to abide by the above.
- I must not use the school e-mail account for selling goods.

- I understand that submitted AI-generated content without appropriate acknowledgement constitutes plagiarism and violates Aldenham Schools' student codes of conduct and acceptable use agreements.

- I understand that the school may use plagiarism detection tools and our academic judgement to identify unacknowledged/plagiarised work.

- I understand that all cases of academic misconduct will be referred to the Deputy Head Academic.

- I understand that misuse of AI tools in the preparation of work for a public examination may have to be reported to the relevant awarding body (examination board) who may take their own disciplinary action up to and including disqualification from the qualification.