Acceptable Use of ICT, Mobile Phones and other Electronic Devices Policy

This policy applies to:

Whole College (including EYFS)

Person responsible for the policy:

Senior Deputy Head,
in consultation with Deputy Head Academic and Director of Digital Strategy & Learning

Review dates:

Last review Sept 2024Next review Sept 2025

Objectives

The College aims to ensure secure access to ICT for all pupils. This policy outlines the acceptable use of internet and electronic communication facilities, file-servers, messaging services, and any networks or hardware, including but not limited to that provided by the College. It applies to any personal devices and other equipment that can be used to access, store or record data or media files.

"Children and young people need to be empowered to keep themselves safe – this isn't just about a top-down approach. Children will be children – pushing boundaries and taking risks. At a public swimming pool, we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim."

Dr Tanya Byron *Safer children in a digital world: the report of the Byron Review*2

The College recognises that social media encourages a new collaborative way of thinking and exploring information with considerable ease. It is important that pupils, parents and staff are able to identify and verify material found on the web for its own worth: they should not be so naïve as to think that information is immune from being inappropriate, biased, bullying or exploitative in nature. It is not enough to impose a list of restrictions; Ardingly College wishes to educate and safeguard pupils, parents and staff on the best use of ICT and alert them to the dangers. The College recognises that the community is no longer bound by the physical campus.

Service Provision

We have excellent network provision, including Wi-Fi from 7am until 11pm, but any issues regarding access should be addressed to ITSupport@ardingly.com . Parents who provide devices with a cellular connection should recognise that these devices can bypass our security and filters (this is addressed in PSHE for students). Some social media sites may be accessed after evening school and under the guidelines outlined in the **Cyber Bullying Policy**.

Ardingly College is not responsible should any mobile device fail. The IT support team can give advice and ensure the fault is not network related but will not attempt any repairs to the physical device or the software running on the device.

Microsoft Surface Pros

All pupils in the Senior School are expected to use a Microsoft Surface Pro, leased by parents directly from our IT Service Provider. Use of a Mobile Device Management system will enable the IT and Senior Leadership teams to remotely distribute updates, settings, and software to the devices. This has the benefit of students not having to source subject-specialist software for their own devices. It will also give parents and teaching staff the peace of mind that pupils are only able to access filtered content and applications and programs that have a clear academic focus.

Students and their parents will be asked to sign usage agreements for the Microsoft Surface Pros before they are issued. The expectations are that students will:

- Look after the Surface Pro and charger very carefully at all times;
- Bring the device to school every day, fully charged and ready for use;
- Always carry it around in the **proper case, with screen protector** so that it is fully protected;

- Take care when it is transported that it is as secure as possible;
- Keep their password and other authentication information a secret from others and ensure the Surface is locked if they walk away.
- Use the Surface to enhance their learning. Examples, but not an exhaustive list, of misuse are:
  - Students must not use the 'chat' function to distract their learning. This will result in a sanction, at least a Friday detention but could be a suspension depending on content of chat.
  - They must not take images or videos of others (students of staff) without their expressed permission. This would result in a serious sanction, most likely suspension, due to potential sharing of unauthorised images.

Networked Computers

Every person using computers connected to the Ardingly College Network has access to a OneDrive folder in order to store personal work. It is expected that students will store all academic files on this platform. Storage areas should not contain any personal data belonging to other staff or students. It is not to be used for personal music, picture files or anything not linked to academic learning or work. Users will be given rights to use certain shared files, networked printers and other resources, as well as internal email. Connection of personal computers to the College LAN is not permitted; however, access via the wireless network is permitted, provided an SSL inspection certificate is installed on all personal devices, enabling the school to filter and block inappropriate web content whilst students are on the College campus. The College's services can be gained wirelessly or at home using the following links:

- Email (Outlook Web Access) https://outlook.office365.com
- ISAMS Pupil portal https://pupils.ardingly.com
- IT Helpdesk itsupport@ardingly.com

Wireless Devices

The College provides a wireless network to all classrooms, boarding and day houses to enable staff and students to access the Internet. Each member of staff or student can have a maximum of three mobile devices connected to the wireless network. Devices can be connected by clicking on the 'Ardingly' WLAN in their list of available networks, installing an SSL certificate, and entering their college username and password. Once connected, there are different levels for Prep, Senior and Sixth Form students in terms of time and web site filtering. Occasional visitors and Summer school clients can be issued with a timed guest pass to enable access to the 'Ardingly Guest' WLAN. Access and expectations are provided and reflect those detailed in this Policy.

Printing

The College has installed print management software, which monitors all printed output. There are currently no restrictions for any users as to the number of copies or number of pages printed. To be as eco-friendly as possible nearly all networked printers are defaulted to print on both sides of a page. It is the responsibility of all users to ensure that the print facilities in College are used in a cost-effective manner. All printed output should be for work related to Ardingly College. Users are not allowed to print any personal documents or images.

Expectations for Acceptable Use of ICT

Cyber-bullying

The College's preventative measures and procedures for dealing with Cyberbullying are detailed in a separate policy available on the College website and on Teams.

Pupils

In relation to ICT, the following are the expectations for pupils while part of the Ardingly College community:

- Pupils must not interfere with the work of others or the system itself by attempting to circumvent the network;

- All academic work submitted using ICT should comply with the College's **Academic Integrity Policy**;

- Pupils must not transmit any messages or prepare files that appear to originate from anyone other than themselves;

- Pupils should not attempt to download and install any software/programs on College devices;

- Pupils must not create, store or send any message internally or externally which is bullying, abusive, humiliating, hostile or intimidating e.g. sharing of nudes or semi-nudes, or posting unpleasant images using Snapchat or any other social media or online platform;

- Pupils will need permission to send messages to large groups of pupils.

Emails

- Pupils should check emails and Teams messages twice a day; this is a College rule.
- Emails, Teams messages or other electronic communication must be composed with courtesy and consideration.

Parents

- Any data which contains information about pupils or staff of Ardingly College should only be published with the College's permission.
- Parents should make every effort to attend lectures about e-safety provided by the College.
- Parents should consider ensuring the appropriate use of technology beyond the School setting.
- Parents who wish to take photographs or video of their child during school events, on or off the Ardingly Campus, should consult the fuller guidance provided in the **Taking, Storing and Using Images of Children Policy**.

College Obligations

Staff are expected to set the example by maintaining the standards of this Policy with particular attention to the following obligations:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive;
- Users must take responsibility for their network use - for Ardingly College staff, flouting the **Acceptable Use Policy** is regarded as a reason for dismissal;
- Workstations should be secured against user mistakes and deliberate actions;
- Servers must be located securely and physical access restricted;
- The server operating system must be secured and kept up-to-date;
- Virus protection for the whole network must be installed and current;
- Access by wireless devices must be proactively managed;
- Resident staff with private Wi-Fi provision must ensure there is no opportunity for students to access their Wi-Fi;
- The College **Data Protection Policy** on Teams must be read and adhered to.

Safe use of personal electronic equipment

It is the responsibility of all staff and students to maintain high security over the information they make available on the internet by using secure sites, high privacy settings and using strong passwords.

They must not disclose passwords to anyone and must not attempt to discover or use the passwords of others. They must take sensible precautions to avoid Internet viruses and should not access sites with age restrictions beyond their years.

No one should put anything onto the web that they would not be prepared for parents, teachers etc. to read. The web is a public forum. Any blog, photograph or personal information posted onto the Internet is there permanently and may be dealt with according to Safeguarding policies. Anything that has been deleted may be cached in a search engine, company server or Internet archive and cause embarrassment years later. Once images are forwarded to others, the same applies.

ICT in the classroom

All Senior School students are expected to bring their Microsoft Surface Pro (and not any other device) to lessons. Students should not use their Surfaces while walking or eating, or at any other socially inappropriate times. They should know where their Surface is at all times and never loan out their Surface to other individuals. It should be labelled with their name and house, in a protective cover, with screen protector and transported in a suitable carrying case. Students are responsible for charging the battery daily, ready for use in lessons. Students should also ensure that they bring their chargers to lessons should they run out of battery.

Surfaces (whether students own in the case of Senior School students or loaned Surfaces in the case of Prep students) should only be used with the teacher’s permission and only for educational purposes during school time. The device should not be used inappropriately, for example for taking personal photographs or browsing the internet recreationally. To reiterate, Surfaces should only be used to enhance learning. Examples, but not an exhaustive list, of misuse:

- Students must not use the ‘chat’ function in Teams to distract their learning. This will result in a sanction, at least a Friday detention but could be a Saturday detention or a suspension depending on content of chat.
- Students must not take images or videos of others (students or staff) without their expressed permission. This would result in a serious sanction, most likely suspension, due to potential sharing of unauthorised images.

They should also be aware that their devices are subject to inspection at any time.

Confidentiality

Any College information or records, including details of pupils, parents and employees, whether actual, potential or past, other than those contained in authorised and publicly available documents, must be kept confidential unless the College's prior written consent has been obtained. This requirement exists both during and after a pupil's time at the College. In particular, pupils or ex-pupils must not use such information for the benefit of any future employer.

Monitoring

The College reserves the right to monitor communications and general network usage in order to:

- Protect pupils;
- Establish facts;
- Prevent or detect crime;
- Investigate or detect unauthorised, suspicious or inappropriate use of College ICT systems;
- Ensure the effective operation of the College network and its systems.

The following checks are in place to assist pupils:

- If there is a suspicion that devices may have been used for illicit activities or contain inappropriate material, the College reserves the right to perform random checks on any device brought into school by pupils;
- The software that allows Internet access through the network maintains a log of all sites visited by all users – this log is kept for inspection;
- Prefects are assigned and have a role to play in educating the wider community in the use of social media;
- Pupils are given a talk about ICT which covers the use of social media, as part of their induction to the College;
- The PSHE programme is also used to help support the work of internet awareness and cyber-bullying;
- The College aims to provide an information evening for parents during the year to discuss the issues of social network sites and access;
- All College staff and pupils must accept the terms of the ICT AUP when logging onto the College network.

Access

Once students are attached to the Ardingly WLAN they can access the Internet via a web filter which requires their standard username and password. Internet access is fully controlled by Internet filtering policies. These policies are designed to protect students from visiting obviously dangerous and unsuitable web sites. The College actively monitors student and staff Internet usage, and has the facility to produce detailed reports by username listing all web sites visited. Students can access emails using Outlook.

Students are expected to only use their Microsoft Surface Pro for all educational activities. Students, of all ages, are not permitted to bring any other devices to lessons - See later guidance (on page 9) regarding mobile phones and wearable technology.

Boarding students may bring additional devices to school, for example a laptop or tablet for the purposes of recreation; however, these must remain in their boarding houses at all times. Students may not have mobile telephones or other devices on their person during the school day (08:20 to

17:30), with the exception of use during break and lunch times in house. During the school day the internet may only be used to access sites and information that is of educational and learning value. Pupils who wish to use sites for difference purposes may only do so with the teacher's permission.

Neither staff nor students should attempt to bypass the College filtering policies by using **virtual private networks**, or any other means. Students found using VPNs, or an equivalent, will be sanctioned, with at a Friday detention but depending on what they are using the VPN to access.

Inspection of machines

As part of the College's safeguarding responsibilities, it may be necessary to inspect a pupil's computer, mobile telephone, or any other device capable of digital recording. The confiscated items are inspected and returned as rapidly as reasonably practicable. If the items contain inappropriate material, that material is wiped from the item's memory, there is likely to be a sanction and a letter will be sent home to the parents. In the event of **sharing of nudes or semi-nude's** (previously known as Youth Produced Sexual Imagery or sexting) being discovered, all devices will be confiscated, and the DSL will be informed as soon as possible.

Education and online safety

The College recognises that blocking and barring sites is no longer adequate in and of itself. It aims to teach all pupils to understand why they need to behave responsibly if they are to protect themselves. Staff professional development is designed to provide educational awareness of online safety. The College makes provision for teaching children to keep themselves safe, including on-line and when accessing remote learning. Online safety considers content, contact, conduct and commerce.

It is essential that children are safeguarded from potentially harmful and inappropriate online material. The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- contact: being subjected to harmful online interaction with other users; for example: child to child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying,
- commerce: - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

This is addressed as part of the PSHE programme at Ardingly; there are key presentations which are followed up in tutorials. The College offers specific external, professional and peer guidance on the safe use of social networking sites, which covers personal security settings and builds resilience. Strong pastoral support is in place to support this work.

Working with parents

The College seeks to work closely with parents and guardians in promoting a culture of e-safety, running evening information sessions on e-safety for parents from time to time. This includes specialist advice about the potential hazards and practical steps parents can take to minimise potential dangers. Communications should be used to reinforce the importance of children being safe online and parents and carers are likely to find it helpful to understand what systems schools and colleges use to filter and monitor online use. The College always contacts parents if there are worries about a pupil's behaviour and encourages parents to share concerns with the College.

Social Use of ICT

The use of social networking sites can be a particular concern for parents and the College alike. Staff and prefects are available to provide informal advice to other students, parents and staff. The College also limits pupils' access to such sites during term time.

Students need to be aware that posting material online (e.g. Social media) regarding a member of staff, without their expressed permission, is taken very seriously and most likely to result in (at least) a suspension from school.

Students need also to be aware that posting material online that is in any way associated with the College that it potentially damaging to the reputation of the school or could identity any member of the school community without their expressed permission can expect to be dealt with swiftly and seriously.

Gaming, films and other video content

The main issues relating to gaming and watching video content are the following:

- The negative impact on work and study ethic;
- Access to games and films that are not age appropriate;
- Their addictive nature;
- The illegal copying of games;
- The difficulties of network access/traffic speed when such media are used;
- The anger and frustration games can evoke in some pupils.

Games, films and other video content may be allowed after evening school and over the weekend at a HoMM’s discretion. Pupils must only watch and play games that are age appropriate. Any material that is not age appropriate will be confiscated and this will be returned to parents at the next opportunity.

Mobile Phones (including wearable technology)

Mobile phones can be used at Ardingly College on the basis that they provide:

- A useful link between parents and their children, especially when arranging transport;
- Communication in an emergency.

The use of mobile phones must not, however, interfere with the working day or the smooth running of the College. The rules relating to mobile phone use at Ardingly College are as follows:

- The College strongly encourages parents NOT to purchase their child(ren) a Smartphone before the age of Year 9. This is in line with the Smartphone Free Childhood national initiative.
- Prep school students are prohibited from having a mobile phone at school, nor are they allowed wearable technology e.g. a Fitbit or watch that has communication facility. This can be highly disruptive to learning. If there is an emergency, the school office should be contacted.
- Students in the **Lower School** (Years 7 & 8) are prohibited from having a phone at school unless:
  a) They are boarding at school that day/evening.
  b) They take the school bus so need to be in contact with parents.
  In these cases, their phone will be securely stored during the school day. Phones must never be used in communal areas of the school.
- For students in the **Middle School** (Years 9 – 11), mobile phones must be switched off and handed in on arrival at school each day, or at the start of the school day for boarding students. They will be stored securely in Houses and can be collected at the end of the school day (17:30 Monday-Thursdays, 16:30 on Fridays). We recommend Day students (whose parents bring them to school) simply do not bring a phone to school. Phones must never be used in communal areas of the school.
- For students in the **Sixth Form** (Years 12 – 13), phones must not be carried on a student's person around the College campus during the school day (08:20 – 17:30). They are welcome to hand their phone in to House staff (following Middle School rules) if they wish. Phones must never be used in communal areas of the school.
- Failure to follow the rules as stated above will result in an instant sanction (Friday detention) and confiscation of the phone for 24 hours, where it will be held by the relevant House staff. Examples of rule breaking include submission of a fake phone when phones are handed in. Repeated breaking of these rules will be escalated in terms of sanctions.
- Using mobile phones to harass or upset other people in any way is an offence punishable by law and by the College;
- Interfering with, hiding or taking someone else's mobile phone will be regarded as theft and quite possibly bullying as well;
- Mobile phones and wearable technology are banned at all times from exam rooms;
- Internet-connected devices (such as phones and wearable technology) should only be used to access the internet at College through the College Wi-Fi, and not through a mobile connection.
- Tracking technology, such as Airtags and other similar products, should not be used at the College or on trips. Use of these products could prevent the detection of unlawful tagging by malicious actors and hinder the College in keeping students safe.

Staff are expected to set the example regarding use of mobile phones and social media although they may provide their school-issued numbers to students for emergency purposes. Personal number sharing should only happen in extreme and emergent circumstances. Staff are aware of the dangers of forming relationships via social media or mobile phones, which are outlined in the **Staff Handbook** and during Child Protection training and should not hold images of students on personal devices. Further information is available in the College's **Social Media Policy** for staff.

Images and Recording

Staff may take and use images or recordings of pupils purely for work purposes but these must not be taken from personal devices. Images suitable for marketing should be saved on the school network, Departmental or House blogs [please do not add surnames to images]. Staff should delete unnecessary or poor-quality images to ensure they stay within storage limits.

Parents have the opportunity to decline the College using images of pupils for promotional purposes. It is recognised that when taking photographs of College events some images may capture pupils other than the intended subject. Where permission has been granted by the Head, parents/guardians should use any personal images with careful consideration for those in the picture and should not publish them on external websites.

Safe use of mobile devices in the Pre-Prep (Farmhouse)

All of the above conditions and expectations apply to staff working in or visiting the Pre-Prep; however, due to the very young age of the children in this part of the College, additional rules must apply, particularly with regard to mobile phones or other devices that may record images.

Young children invest a great deal of trust in adults, particularly those in positions of authority, and are unlikely to question their actions even if the actions make the child feel uncomfortable or unhappy. Very young children may not have the understanding to know when something is inappropriate or the vocabulary to express their concerns. It is therefore very important that we have in place mechanisms to protect them.

No member of staff working in, or visiting, the Pre-Prep School or Nursery should have their mobile phone out and in use near children during the working day (i.e. when children are still on site).

Mobile phones should be stored out of sight of the children and only accessed during recognised break times in an area where there are no children, such as the staffroom. Staff, pupils visiting the Pre-Prep and any other visitors to the site should keep any mobile devices out of sight and not use them in the presence of children. The school provides devices (e.g. Surface Pros, cameras or iPads) for the recording of images of children and only these devices may be used for this purpose. The intention is to provide protection for the children. There may be the opportunity for parents to take photographs at official events [sports day, celebration assembly, Christmas play] but under no circumstances should personal mobiles, personal iPads or other mobile devices be used to take images of children outside of these events or without permission. All staff, pupils and any other person visiting the Pre-Prep are required to comply with this regulation.

Reporting

Technical issues should be reported to itsupport@ardingly.com. A breach of **ICT Code of Conduct** should be reported to the appropriate member of staff, usually the HoMM or line manager.

Sanctions

In the event of any breach of the policy, appropriate sanctions are imposed: these may range from confiscation of any personal or shared devices to more serious sanctions, including exclusion, depending on the activity. If the breach is of a criminal nature, the Police and Local Safeguarding Children's Board (LSCB) may be involved. If the College discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). The DSL handles all Child Protection situations.

Pupils and parents sign a contract agreeing to **Acceptable Use of ICT** at Ardingly College.

Confiscated equipment must be returned to the HoMM where it will be safely stored before being returned to the pupils or parents.

This policy should be read in conjunction with the following additional College policies, Government guidance and further online resources:

- **Safeguarding Policy**
- **Cyberbullying Policy**
- **Anti-Bullying Policy**
- **Behaviour and Conduct Policy**
- **Professional Code of Conduct for Staff**
- **Social Media Policy**
- **Data Protection Policy**
- **Taking, Storing and Using Images of Children Policy**
- **AI policy**

- DfE advice on preventing and tackling and bullying, including cyberbullying: https://www.gov.uk/government/publications/preventing-and-tackling-bullying
- Current government advice on sharing nudes/semi-nude images: https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people
- Childnet International (www.childnet-int.org)
- Digizen (www.digizen.org.uk)
- Cyber Mentors (www.cybermentors.org.uk)
- E-Victims (www.e-victims.org)
- Bullying UK (www.bullying.co.uk)