2026

Al Zahra College Acceptable Use of ICT Policy

Al Zahra College – Acceptable ICT Use Policy & Student Agreement

1. Policy

This policy guides the responsible and ethical use of Information and Communication Technologies (ICT) at Al Zahra College. This ensures a safe, respectful, and distraction-free environment that supports student learning and wellbeing, while aligning with Islamic values and IB learner profile attributes.

The purpose of this policy is to:
- Foster integrity, privacy, and digital citizenship
- Promote safe and effective use of digital devices and platforms
- Protect students and staff from harmful content and digital misuse
- Ensure compliance with legal and duty-of-care obligations.

2. Implementation

2.1 This policy applies to all students, parents, stakeholders and school visitors; pertaining to the use of digital devices, including school-owned or BYOD (Bring Your Own Device) technology, whether on school grounds, during off-site events, excursions, or while engaging school-related digital platforms.

2.2 Mobile phones and smartwatches are strictly prohibited during school hours, including class time, breaks, excursions, off-site events or camps (unless specifically authorised), and during in-school extracurricular activities.

2.3 Students may use **one** BYOD-approved educational device only.

2.4 The use of VPN (Virtual Private Networks) or proxy tools to bypass school internet filters is a serious breach of school ICT policy. Under no circumstances should a student ever use a VPN at school.

2.5 Students must demonstrate digital safety practices and responsible cyber conduct.

2.6 All software used must be legally obtained and licensed.

2.7 By signing the AZC Use of ICT Agreement form, students and parents/guardians agree to: follow the Al Zahra College Acceptable ICT Use Policy; accept all outlined rules, expectations, and consequences; and promote safe and responsible digital use aligned with school values.

3. Evidence

3.1 Breaches Register: VPN, phones.

3.2 Digital Safety and Cyber Conduct Register.

Updated: November 2026

Review: November 2027

SUPPORTING STATEMENTS

1. Digital Principles

Al Zahra College upholds the following digital principles:

- **Privacy:** Respect the personal data, images, and digital presence of others.
- **Integrity:** Use technology ethically and never engage in plagiarism, impersonation, or deceit.
- **Safety:** Avoid harmful sites and unsafe digital communication. Report suspicious content immediately.
- **Learning:** Use devices strictly to assist in learning and learning associated tasks. Devices are not to be used for gaming, entertainment, and other uses that distract from learning during school hours.
- **Respect:** Treat digital spaces as extensions of the classroom - free of bullying, harassment, or disruption.
- **Ownership:** Honour intellectual property rights and digital integrity in adherence with copyright laws.

2. Mobile Phone & Smartwatch

The following rules in relation to mobile phones and smart watches apply to all students:

- Mobile phones must be stored in the designated phone lockers for the duration of the day.
- Collection is allowed only at the end of the day, after the school bell has rung.
- Smartwatches with communication, camera or internet functions are treated the same as phones.

Breaches will result in:

- First Offence: 1-day suspension + device collected by parent/guardian
- Second Offence: 1-week suspension
- Third Offence: Enrolment review

Note: Students on approved Flexi-Leave (off school premises) are exempt during their leave periods only.

3. Laptop & Device Use

School device usage must align with the following rules:

- Devices must be charged at home and be classroom ready each day.
- Devices are to be used for learning only.
- AirPods (as well as any other wireless earbuds) are strictly not allowed during school hours. (**Consequence:** AirPods will be confiscated and student will be placed on afternoon detention)
- Headphones/earphones may only be used when a teacher explicitly allows them for a task.
- All passwords must remain confidential and secure. No student is to share or provide his/her school-account login details with any other unauthorised person.

Students must not:
- Play games on their devices during class
- Stream videos or access YouTube (unless required for learning, and approved by the class teacher)
- Access social media platforms, or messaging apps during school hours
- Alter security settings or attempt to "hack" school filters
- Create ad-hoc networks or connect their devices to unauthorised WIFI networks (including attempting to connect to the staff WIFI network).

Failing to adhere to these rules will result in the student losing network access.
Additional consequences may include:
- After-school detention
- Suspension
- Network exclusion.

Multiple failures will result in more severe consequences, such as an extended network exclusion, and possible expulsion.

4. VPN Use

Any VPN use will result in the following consequences:

1st Offence – 1-day network exclusion
2nd Offence –1-week network exclusion
3rd Offence – 1-month network exclusion + enrolment review.

**Device exclusion means the student will not be able to access the internet or school data network from his/her device.*

This protects our safe and secure learning environment and ensures all internet use is monitored for safety.

Note: No student should have a VPN installed on their school device. If there is a reason for them to use a VPN at home, the VPN should be uninstalled before bringing their device to school.

5. Digital Safety & Cyber Conduct

Students must <u>never</u>, whether at school or off school premises:

- Record or photograph staff or students without permission
- Send or share inappropriate, offensive, or suggestive content
- Post or engage in cyberbullying, threats, or harassment
- Pretend to be someone else online or use anonymous accounts while communicating with other students or staff
- Access or distribute adult or violent content.

Violations may lead to:
- Immediate network/device exclusion
- Formal suspension
- Police involvement (for severe incidents)
- Enrolment review in serious or repeated cases

6. Respecting Copyright, Software & Ownership

All software used must be legally obtained and licensed.
Students must not:

- Attempt to download pirated files, games or music using the school network
- Share copyrighted textbooks, PDFs, or eBooks without permission
- Plagiarise or copy content from the internet without proper citation.

7. Roles and Responsibilities

Students must:

- Follow all rules outlined in this policy
- Use their devices for learning only
- Respect others' privacy and wellbeing online
- Be willing to accept all consequences if breaching any part of this policy
- Report any cyber safety concerns or access issues to their teacher who may escalate it to the school IT Department.

Parents / Guardians are expected to:

- Support the College's expectations at home
- Monitor online use and device activity outside school
- Communicate with staff regarding concerns
- Reinforce safe digital behaviours.