DOHA COLLEGE

ICT AND INTERNET ACEPTABLE USE POLICY (staff and students)

W04

Policy owner:	**Vice Principal - Curriculum**
Policy agreed on:	**September 2010**
Policy reviewed on:	**June 2022**
Policy to be reviewed on:	**June 2025**

DOCUMENT CONTROL TABLE

Status	Live
Policy owner	Vice Principal - Curriculum
Statutory/Recommended	Recommended
Date approved	September 2022
Review period	3years
Latest review date	June 2022
Next review date	June 2025
Linked documents and policies	Behaviour Policy Safeguarding Policy Data Protection Policy Online safety Remote learning Policy Social Media
Date	**Comments**
November 2015	Location of IT Office
February 2020	Amendments in policy section Added in 'Student use of iPads' Added in 'Digital Learning at Doha College'
February 2022	Full review of entire policy

KEY CONTACTS

Executive Designated Safeguarding Lead	Uzma Zaffar (EDSL)	**Contact details**	uzaffar@dohacollege.com Office: 44076705 (Ext:705) **Emergency Number: 856**
Designated Safeguarding Lead for Primary	Danielle Price (DSL)	**Contact details**	dprice@dohacollege.com Office: 44076777 (Ext: 768)
Designated Safeguarding Lead for Secondary	Nicholas Taylor (DSL)	**Contact details**	ntaylor@dohacollege.com Office: 44076761 (Ext:761)
Designated Safeguarding Governor	Lisa Ethridge	**Contact details**	liethridge@dohacollege.com

Principal	Martin George	**Contact details**	mageorge@dohacollege.com Office:44076700

TERMINOLOGY

Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programs designed to self-replicate and infect legitimate software programs or systems.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
ICT facilities	includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
Users	anyone authorised by the school to use the ICT facilities, including governors, staff, students, volunteers, contractors, and visitors
Personal use	any use or activity not directly related to the users' employment, study, or purpose
Authorised personnel	employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
Materials	files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

CONTENTS

AIMS

Information and communications technology (ICT) is an integral part of the way Doha College works, and is a critical resource for students, staff (including leadership teams), governors, volunteers, and visitors. It supports teaching and learning, pastoral, and administrative functions of the school.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety, and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, students, parents, and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching students safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, students, volunteers, contractors, and visitors.

Breaches of this policy may be dealt with under our disciplinary policy, behaviour policy and/or the student/staff code of conduct.

RELEVANT LEGISLATION AND GUIDANCE

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2021
- Searching, screening and confiscation: advice for schools

- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

In addition to these it also seeks to.

Abide by all local and applicable laws, regulations, and policies such as the Qatar Cybercrimes Law (Law 14 of 2014).

UNACCEPTABLE USE

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Removing the MDM from devices manually or using a VPN to block access to the iPad when in school
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or live streams (also known as sexting or youth-produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its students, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel

- Setting up any software, applications, or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts, or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting, or disposing of ICT equipment, systems, programs, or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic, or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Principal, members of the leadership group and/or any other relevant member of staff will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

Exceptions from unacceptable use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Principal's discretion. This needs to be done in writing and clearly outline the rationale behind this request.

Sanctions

Students and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on behaviour, staff discipline and the staff and/or student code of conduct.

STAFF (INCLUDING GOVERNORS, VOLUNTEERS, AND CONTRACTORS)

Access to school ICT facilities and materials

The school's Head of IT manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones, and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Head of IT.

Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only. Staff must enable multi-factor authentication on their email accounts.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and students and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from

a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the Head of IT immediately and follow our data breach procedure.

Staff should not use their DC email address for any personal activities such as registering on online sites

Staff shall not make offline copies of their mailboxes which may expose them to unauthorized disclosure.

Staff so not have the right to take copies of their email when their association with Doha College ends

Staff must not give their personal phone numbers to parents or students. Staff must use phones provided by the school to conduct all work-related business.

Doha College owns the content of electronic mailboxes of its students and staff and all other mailboxes created to facilitate Doha College business, e.g., consultants and contractors.

The Information Technology Department (IT) is responsible for managing and supporting Doha College's email services.

IT may provide access to, or copies of the content of, mailboxes as required by Doha College and/or during an investigation.

Email accounts may be disabled: e.g., when an employee's association with Doha College ends.

Exceptions may be granted for a specified period of time if such access is required to fulfil a business need or if they are linked to security incidents such as SPAM or other inappropriate use of email.

School phones should not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. Members of the leadership group may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during teaching time.
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no students are present
- Does not interfere with their jobs, or prevent other staff or students from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where students and parents could see them.

Staff should take care to follow the school's guidelines on social media and use of email to protect themselves online and avoid compromising their professional integrity.

Personal social media accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

Remote access

We allow staff to access the school's ICT facilities and materials remotely. They should dial in using a virtual private network (VPN).

They can log in to the VPN using their DC network username and password.

They can connect to the VPN using the link https://vpn.dohacollege.com

The IT Department manages the remote access system. Staff can request this facility by sending an email to IT Help Desk

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the Head of IT may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

School social media accounts

The school has official Facebook, Twitter, and LinkedIn pages, managed by the Marketing department and overseen by the Director of Marketing and Communication. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

More guidance can be found in the Social Media Policy.

Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record, and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures, and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation.

Use of Imaging Devices (Printers, Scanners, Copiers)

- Printing, scanning, and copying devices and materials provided by Doha College are the sole property of Doha College and should be used for school business only.

- Users should consider the surroundings when printing or copying confidential information and should promptly remove the printed material from the printer.

Users shall not:

a. attempt to move or remove printers and scanners from their locations without prior consent of ITS;
b. attempt to fix a printer or scanner without contacting the IT Help Desk for support;
c. print or distribute abusive, offensive, or unethical material.

Telecommunication Service (Telephones)

Doha College uses IP phones (hardware and software) to provide telephone services to its staff.

Users:

- Should handle the phones with care and report any hardware or configuration issues to the ITS Help Desk
- Should protect their phone PIN, especially if they have access to make long distance calls
- Must not abuse their long-distance access privileges. Reported abuses may result in disciplinary action
- Use phones that are distributed around campus for emergency purposes only

Google

Users of the shared file storage services must comply with the following:

Departmental Shared Drives:

Departments are responsible for the access authorisation and for the content of their assigned shared folders.

Departmental shared drives must undergo periodic reviews to ensure that the content is valid, and that access control is properly set. The IT department can assist in such tasks but cannot be held responsible for any unexpected findings.

Departmental shared Drives should not be used to back up individual user documents.

Individual Shared Drives

Users of individual shared drives must not store any illegal or inappropriate content.

To ensure the security of the content stored in individual shared Drives should back up their content to off-line storage devices. The IT department cannot guarantee that such content is backed up to central backup facilities.

Maintenance of Clear Screen

Staff shall maintain a clear screen on their desktops/laptops by:

- Activating the screen saver on their PC/desktop/laptop/netbook
- Configuring the screen saver to:
    a. lock the screen if the system is idle for more than 5 minutes require a password to resume operation
- Not tampering with the screensaver settings enforced by IT

STUDENTS

Access to ICT facilities

The following ICT facilities are available to students:

- Computers and equipment in the school's ICT suite are available to students only under the supervision of staff
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff
- Students in KS2, KS3 and KS4 are expected to have a suitable iPad to use in school.
- Students in KS5 can choose to use an iPad or personal laptop.
- Students will be provided with a Google account which they can access from any device by using a Doha College email address and password.
- All students can use the computers in the library under supervision.
- All ios devices are monitored and controlled by the JAMF MDM and all personal laptops have their M.A.C address logged on the system.

Search and deletion

Under the Education Act 2011, and in line with the Department for Education's **guidance on searching, screening and confiscation,** the school has the right to search students' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

Staff members may also confiscate devices for evidence to hand to the police, if a student discloses that they are being abused and that this abuse contains an online element.

Unacceptable use of ICT and the internet outside of school

The school will sanction students, in line with the behaviour policy, if a student engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other students, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel

- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

PARENTS

Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with the school in an official capacity (for instance, as a volunteer or as a member of the FDC) may be granted an appropriate level of access or be permitted to use the school's facilities at the Principal's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

Communicating with or about the school online

We believe it is important to model for students, and help them learn how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents to sign the agreement in appendix 2.

DATA SECURITY

The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data, and user accounts. However, the school cannot guarantee security. Staff, students, parents, and others who use the school's ICT facilities should use safe computing practices at all times.

Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or students who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

- All staff can use Classlink to help them store their passwords to various sites securely.
- Staff can also use Chrome's password storage facility.
- For staff and students, most applications and programmes used in school have been configured to accept Google Single Sign on, and where this is not possible - separate passwords have been generated and distributed to students.

Software updates, firewalls, and anti-virus software

All the school's ICT devices that support software updates, security updates and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical, and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files, and devices.

These access rights are managed by the Head of IT.

Users should not access, or attempt to access, systems, files, or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Head of IT immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers, tablets, and USB drives) to access school data, work remotely, or take personal data (such as student information) out of school if they have been specifically authorised to do so by the Principal or Heads of School.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the Head of IT].

PROTECTION FROM CYBER ATTACKS

Please see the terminology to help you understand cyber security terminology.

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
- Check the sender address in an email
- Respond to a request for bank details, personal information, or login details
- Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents

- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data

Put controls in place that are:

- **'Proportionate'**: the school will verify this using a third-party audit to objectively test that what it has in place is up to scratch
- **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
- **Up to date:** with a system in place to monitor when the school needs to update its software
- **Regularly reviewed and tested**: to make sure the systems are as up to scratch and secure as they can be
- **Back up critical data** regularly and store these backups on [cloud-based backup systems/external hard drives that aren't connected to the school network and which can be stored off the school premises]
- **Delegate** specific responsibility for maintaining the security of our management information system (MIS) to our IT department.
- Make sure staff:
- Dial into our network using a virtual private network (VPN) when working from home
- Enable multi-factor authentication where they can, on things like school email accounts
- Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and seeing if they have the **Cyber Essentials** certification
- Develop, review, and test an incident response plan with the IT department, for example, including how the school will communicate with everyone if communications go down, who will be contacted when, and who will notify any appropriate external bodies. This will be reviewed and tested frequently, and after a significant event has occurred, and the risk register updated.

INTERNET ACCESS

The school wireless internet connection is secured.

In addition, we also have:

- Filtering
- Separate connections for Staff, students, and Guests where appropriate

Students

- Wi-Fi is available in the following ways to students every school day
- Wi-Fi is only available to iOS devices that have JAMF MDM installed for KS2, 3 & 4 and registered laptops for KS5
- Students can access the guest Wi-Fi before and after school using their DC login details - this is to allow arrangement of transport and to contact home if needed
- Personal devices cannot connect to the student network during the school day.
- Wi-Fi is monitored by JAMF for KS2, 3 & 4 and firewall settings for KS5.
- EYFS and KS1 access the Wi-Fi through school iPads that connect to the student Wi-Fi.

PARENTS AND VISITORS

Parents and visitors to the school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by members of the leadership group.

This authorisation will only be granted if:

- Parents are working with the school in an official capacity (e.g., as a volunteer or as a member of the FDC)
- Visitors need to access the school's Wi-Fi to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)
- Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

MONITORING AND REVIEW

The Vice Principal - Teaching and Learning in collaboration with the Heads of Digital Learning and the Head of IT monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

APPENDIX 1

Facebook cheat sheet for staff

If you have a social media policy, adapt this in line with that policy. You may decide to hand this cheat sheet out to your staff as a standalone document and remove it from here. If so, renumber

Don't accept friend requests from pupils on social media

the following appendices and check for references to appendix 1 in the policy.

10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your students
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school, or your students online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g., by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connection (such as parents or students)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, students and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if…

A student adds you on social media

- In the first instance, ignore and delete the request. Block the student from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the student asks you about the friend request in person, tell them that you're not allowed to accept friend requests from students and that if they persist, you'll have to notify senior leadership and/or their parents. If the student persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

It is at your discretion whether to respond. Bear in mind that:

Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school

students may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in

If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

Do not retaliate or respond in any way

Save evidence of any abuse by taking screenshots and recording the time and date it occurred

Report the material to Facebook or the relevant social network and ask them to remove it

If the perpetrator is a current student or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents

If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material

If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

APPENDIX 2

Acceptable use of the internet: agreement for parents and carers

The below will be generated and sent electronically for digital approval at the beginning of the academic year.

Acceptable use of the internet: agreement for parents and carers
Name of parent/carer: **Name of child:**
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: ● Our official Facebook page ● Our official Twitter account ● Email/text groups for parents (for school announcements and information) ● Our virtual learning platform Firefly ● Through Google Classroom Guardian Summaries Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: ● Be respectful towards members of staff, and the school, at all times ● Be respectful of other parents/carers and children ● Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure I will not:

● Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive, and the school can't improve or address issues if they aren't raised in an appropriate way ● Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other students. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident ● Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers	
Signed:	**Date:**

APPENDIX 3

Acceptable use agreement for Secondary students

The below will be generated and sent electronically for digital approval at the beginning of the academic year.

Acceptable use of the school's ICT facilities and internet: agreement for students and parents/carers
Name of student:
When using the school's ICT facilities and accessing the internet in school, I will not: ● Removing the MDM from devices manually or using a VPN to block access to the iPad when in school. ● Use them for a non-educational purpose ● Use them without a teacher being present, or without a teacher's permission ● Use them to break school rules ● Access any inappropriate websites ● Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) ● Use chat rooms ● Open any attachments in emails, or follow any links in emails, without first checking with a teacher ● Use any inappropriate language when communicating online, including in emails ● Share any semi-nude or nude images, videos, or live streams, even if I have the consent of the person or people in the photo ● Share my password with others or log in to the school's network using someone else's details ● Bully other people ● Do not use the network in anyway that might disrupt the service for others ● Plagiarise other's work online and claim it as my own

- Vandalise harm or destroy any equipment or data of another user, or of any other networks that are connected to the system. This includes but is not limited to: the uploading or creation of computer viruses, the wilful damage of computer hardware, whether connected to the network or not, the deletion of data from its place of storage or damaging another person's iPad/ personal computer.

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (student):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

APPENDIX 4

Acceptable use agreement for Primary students

The below will be sent as a paper copy at the beginning of the academic year.

Acceptable use of the school's ICT facilities and internet: agreement for students and parents/carers
Name of student:
When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not: ● Use them without asking a teacher first, or without a teacher in the room with me ● Removing the MDM from devices manually or using a VPN to block access to the iPad when in school ● Use them to break school rules ● Go on any inappropriate websites ● Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson) ● Use chat rooms ● Open any attachments in emails, or click any links in emails, without checking with a teacher first ● Use mean or rude language when talking to other people online or in emails ● Send any photos, videos, or live streams of people (including me) who aren't wearing all of their clothes ● Share my password with others or log in using someone else's name or password ● Bully other people I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules. I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the school's ICT systems and internet. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	
Signed (student):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

APPENDIX 5

Acceptable use agreement for staff, governors, volunteers, and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers, and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal, or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its students or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a student informs me, they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that student s in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

DOHA COLLEGE

Accredited by

BSME BRITISH SCHOOLS IN THE MIDDLE EAST | Accredited Member

British School Overseas BSO Inspected

CIS WE ARE AN ACCREDITED SCHOOL

The Patron's ACCREDITATION AND COMPLIANCE ACCREDITED

HPL Membership Network

Eco-Schools

About Doha College

Vision

To enable personal growth, instil a passion for learning and create aspirational minds.

Mission

With the growth-mindset philosophy of High Performance Learning, we develop confidence, creativity and intellectual curiosity in a safe, caring and inclusive environment for our students to make a lasting contribution to global society.

Core Values

Excellence and diligence
Respect and Integrity
Commitment and Accountability
Perseverance and Honesty
Fun and Enjoyment
Challenge and reward

Doha College
PO Box 7506,
Doha, State of Qatar

+974 4407 6777
enquiries@dohacollege.com
www.dohacollege.com

A BRITISH INTERNATIONAL SCHOOL