

Online Safety Policy

Contents

1. Introduction and Aims.....	1
2. Legislation and guidance.....	2
3. Roles and responsibilities.....	3
4. Educating pupils about online safety.....	6
5. Educating parents/carers about online safety.....	7
6. Cyber-bullying.....	8
7. Acceptable use of the internet in school.....	10
8. Pupils using mobile devices in school.....	11
9. Staff using work devices outside school.....	11
10. How the school will respond to issues of misuse.....	11
11. Training.....	12
12. Monitoring arrangements.....	12
13. Links with other policies.....	13
Appendix 1: Acceptable use agreement (pupils and parents/carers).....	14
Appendix 2: Acceptable use agreement (staff, governors, volunteers and visitors).....	16
Appendix 3: Online safety incident report log.....	17

1. Introduction and Aims

At Dubai College, we are committed to ensuring the safety and well-being of our students in all aspects of their education, including their online interactions. As the digital world becomes an integral part of learning and communication, it is crucial that we prioritise online safety to protect our students from potential risks while empowering them to use technology responsibly. Our Online Safety Policy aims to provide clear guidelines for students, staff, and parents, fostering a secure digital environment that supports safe online practices, promotes digital literacy, and encourages respectful

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer 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** – personal online behaviour that increases the likelihood of, or causes, harm, such as 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; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

UK

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#) – applying sensitivity to cultural values to the content covered
- [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

UAE

This policy also considers the Law on combatting rumours and cybercrimes, Federal Decree Law No. 34 of 2021 on Combatting Rumours and Cybercrimes which took effect on 2 January 2022. The law provides a comprehensive legal framework to address the concerns relating to the misuse and abuse of online technologies.

And Federal Decree Law No. 45 of 2021 Regarding the Protection of Personal Data, also known as the Personal Data Protection Law constitutes an integrated framework to ensure the confidentiality of information and protect the privacy of individuals in the UAE. It provides proper governance for data management and protection and defines the rights and duties of all parties concerned.

It also links to UAE documentation on Child Digital Safety and Protection of children's data online.

The Ministry of Interior and the National Programme for Happiness and Wellbeing launched the 'Child Digital Safety' initiative in March 2018, in a joint effort to raise awareness among children and school students about online threats and challenges and promote a safe and constructive use of the internet.

Article 29 of Federal Law No. 3 of 2016 Concerning Child Rights, also known as [Wadeema's Law](#) (PDF, 250 KB), states: The telecommunications companies and internet service providers shall notify the competent authorities or the concerned entities of any child pornography materials being circulated through the social media sites and on the Internet and shall provide necessary information and data on the persons, entities or sites that circulate such material or intend to mislead the children.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet their safeguarding needs

The governor who oversees online safety is as part of his safeguarding role is Graham Lovett.

All governors will:

- Ensure they have read and understand this policy

- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 1)
 - Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
 - Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 Educational Systems Director team and the ICT manager

The ESD and ICT manager are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems monthly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy (DH:P)

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 1), and ensuring that pupils follow the school's terms on acceptable use
- Knowing that the DSL is responsible for checking the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by Dubai College
- Following the correct procedures by alerting the ICT manager if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#)
- Hot topics – [Childnet](#)
- Parent resource sheet – [Childnet](#)
- [CEOP](#) - National Crime Agency's CEOP Education

Parents are offered the opportunity to access course developed by National Online Safety as part of The National College suite of course. All parents can find the necessary links on the slide deck from the information to the year evening.

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

The education programme at Dubai College is based on:

- [Relationships and sex education and health education](#) in secondary schools
- Educated for a Connected World - a framework for online education linked to KCSiE.

In **KS3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **KS4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents/carers about online safety

Dubai College will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website and through the parent portal. This policy will also be shared with parents/carers. Online safety will also be covered during the information to the year evenings at the start of the academic year.

Dubai College will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online and how

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour and sanctions policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

Dubai College actively discusses cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff are encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes through the RPEP curriculum which encompasses culturally sensitive aspects of the UK personal, social, health and economic (PSHE) education, relationships and sex education (RSE) and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of Dubai College's online safeguarding training (see section 11 for more detail). In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour and sanctions policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Assess how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#), the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#) and any local UAE legislation and latest guidance.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Our behaviour and sanctions policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard for example.

Dubai College recognises that AI has many positive uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Dubai College will treat any use of AI to bully pupils in line with our anti-bullying and behaviour and sanctions policies.

Staff are made aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the Dubai College. It is crucial to consider data protection in this context. AI tools often require access to large datasets, which may include sensitive information about pupils, staff, and other stakeholders. Ensuring that this data is handled according to data protection laws and guidelines is essential to safeguard privacy and prevent misuse.

The college implements robust data protection policies and practices to ensure that any data used or generated by AI tools is secure. This involves encrypting data, restricting access to authorised personnel only, amongst others.

Approval must be sought by teachers wanting to use AI for workload reduction purposes before their implementation. This allows the school to evaluate any potential data protection risks and address them proactively. By integrating data protection considerations into the risk assessment for AI tools, we can mitigate privacy concerns and ensure a safe and ethical use of technology.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected read, understand and abide by the rules regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors (including subcontractors) will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

Pupils may bring mobile devices/smart phones into school but should not be seen or switched on inside the campus between stepping within the campus perimeter after morning drop off until after 4:45pm. Please see the mobile policy for more granular detail.

Students can use laptops/surface pros for educational purposes during lessons and supervised free time at break and at lunch time.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 2.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from IT Support: Team Leader.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate along with the sanctions aligned within the behaviour policy.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required through emails, MS Staffroom Team (safeguarding) and in staff meetings/briefings.

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, threatening, harassing and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills about online safety at regular intervals, and at least annually. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 3.

The policy will be shared with the governing board and cross checked by the link governor at Education Subcommittee meetings. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding and child protection policy
- Behaviour and sanctions policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Review of Policy

The bullying policy is monitored by SLT and reviewed on an annual basis.

Policy Details	
Version date	September 2025
Last review	October 2024
Next review	September 2026
Responsible SLT	Deputy Head: Pastoral & DSL

Appendix 1: Acceptable Use Agreement (pupils)

ICT, including the internet, email, mobile technologies and online resources have become an important part of learning in our college. We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of Online Safety and know how to stay safe when using any ICT.

Students are expected to read and discuss this agreement with their parent(s) and follow the terms of agreement at all times. Any concerns or explanations required should be discussed with the Educational Systems Director.

GENERAL

- I will only use ICT systems in college, including the internet, e-mail, digital video, and mobile technologies for college purposes
- I will not download or install software on college technologies
- I will only log on to the college network, other systems and resources with my college supplied username and password and will only use my own device or college provided technology
- I will follow the college's Cybersecurity policy and not reveal my passwords to anyone and will change them regularly
- I will only use my college e-mail address for college purposes, including communication with teachers and staff
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible
- I will be responsible for my behaviour when using the internet. This includes resources I access and the language I use
- I will not browse, download, upload or forward material that could be considered offensive or illegal.
- I am aware that when I take images of other students and/or staff, that I must only store and use these for college purposes in line with college policy and must never distribute these outside the college network without the permission of all parties involved. This includes college breaks and, on all occasions, when I am in college uniform or when otherwise representing the college
- I will ensure that my online activity, both in college and outside college, will not cause the college, staff, students or others distress or bring the college community into disrepute, including through uploads of images, video, sounds (including voice recordings) or texts
- I will support the college approach to online safety and not upload or add any images, videos, sounds (including voice recordings) or texts that could upset any member of the college community
- I will respect the privacy and ownership of others' work online at all times and use appropriate forms of referencing to credit my sources of information accordingly. I will not plagiarise and pass off someone else's work as my own; this includes the use of AI technologies
- I will not attempt to bypass the internet filtering system using any methods
- I understand that all my use of the internet and other related technologies, either on my own device or on a college provided technology, can be monitored and logged and can be made available to staff or other appropriate authorities
- I understand that these rules are designed to keep me safe and if they are not followed, college sanctions will be applied, and my parent will be contacted
- I will not sign up to online services until I am old enough to do so

Additional Agreement for Personal Devices (under the BYOD Scheme) and Mobile/Smartphones

- I understand that devices should not be used during normal college hours for personal texting, e-mail, online shopping, live streaming or downloading of any non-educational material
- I will ensure that my devices are connected to the Dubai College Wi-Fi network always. (Using any other network or use of hotspots is strictly prohibited)
- I will take full responsibility for my device and will not leave it at college overnight.
- I will immediately comply with teachers' or staff requests to shut down my device or close the screen when instructed
- I understand that intentionally infecting the network with a virus, Trojan or program designed, alter, destroy, or provide access to unauthorised data or information will result in disciplinary actions. Suitable virus protection software is required
- I will use my device at college for educational purposes only, accessing files or internet sites relevant to the classroom curriculum and supported by specific subjects and teachers
- I understand that devices may not be used between lessons, at break times or in college buildings at any time outside of normal lessons unless directed by college staff.
- I understand that any member of college staff reserves the right to ask me to show them what I have been accessing on my device
- I will ensure that I come to college with my device fully charged daily
- I have read and understand the additional rules for use of my Mobile or Smartphone (available on DC website)

Disciplinary Procedures

- The understanding of both student and parent is that the use of personal devices, to support educational experiences, is a privilege. When expectations are abused, or the above agreement is violated such privileges may be withdrawn and additional disciplinary actions may result.
- This acceptable use agreement should be read in conjunction with the Mobile Phone Policy and the Use of Dubai College ICT Systems Policy (available on the college website) and constitutes part of the school's Behaviour and Sanctions Policy.
- Those who violate this Acceptable Use Policy will be subject to disciplinary procedures. Violations may result in disciplinary action up to and including suspension or expulsion for students. When applicable, law enforcement agencies may be involved after consultation with the KHDA.
- Acceptance (via a Microsoft form) of this agreement is part of the Year 7 induction process. Parents confirm that they have read, understood, and discussed this with their child before their first day at Dubai College as part of the ICT onboarding process

Appendix 2: Acceptable Use Agreement (staff/governors/visitors (including parents and volunteers))

Staff, governors and visitors are expected to read, understand and abide by the rules listed in this document.

Any concerns or explanations required should be discussed with the Educational Systems Director.

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), 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 that could harm the school's reputation
- Access social networking sites or chat rooms for personal use
- 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
- Take photographs/video of pupils without checking with teachers/staff first
- Share confidential information about the school, its pupils 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 will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.
- I agree 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 Educational Systems Director know if a pupil informs me they have found any material that 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 pupils in my care do so too.

Appendix 3: Online Safety Incident Report Log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident