



Durham School Dubai

Confidence for Life

Online Safety Policy

Updated: August 2026

Review: August 2027

CONTENTS

1 Introduction	3
2 Aims and Objectives	3
3 Acceptable Use of Technology	4
3.1 Pupil Expectations	4
3.2 Staff Expectations	4
3.3 Pupil Mobile Phones	5
4 Online Safety Rules for Staff	5
4.1 Monitoring and Security	6
5 Personal Devices	6
5.1 Mobile Phones	6
5.2 Smartwatches and Tablets	6
5.3 Photography and Video	7
6 Social Media and Professional Boundaries	7
7 Cyberbullying	8
8 Online Child Protection Risks	9
8.1 Content	9
8.2 Who to Contact	9
8.3 Conduct	9
8.4 Commerce	10
8.5 AI	10
9 Responding to Online Safety Concerns	11
10 Filtering and Monitoring	11
10.1 Authorising Internet Access	11
10.2 Assessing Risks	11
10.3 Online Safety Complaints	12
11 Data Protection, Privacy and Confidentiality	12
11.1 Confidentiality and Safeguarding	12
11.2 Communications	12
12 Parents' Support	13
13 Online Safety Incidents: Recording and Reporting	13
14 Parents and Carers	14
15 Policy Information	14

1 Introduction

Online safety encompasses the use of internet technologies and electronic communications, including mobile phones, wireless technology and other digital devices. Technology plays an important role in the education and development of children and young people and provides many opportunities for learning, communication and collaboration. However, Durham School Dubai recognises the risks associated with the use of technology and is committed to providing appropriate safeguards, education and support to help pupils use technology safely and responsibly.

The Durham School Dubai Online Safety Policy operates alongside UAE Federal Law and other relevant school policies, including the Safeguarding and Child Protection Policy, Behaviour Policy and Anti-Bullying Policy.

The policy reflects the requirements of Keeping Children Safe in Education (KCSIE) and recognises the importance of effective filtering and monitoring of school devices and networks as part of the school's safeguarding arrangements.

The policy has also been developed with regard to the Ministry of Interior and National Programme for Happiness and Wellbeing 'Child Digital Safety' initiative, which aims to raise awareness among children and young people about online threats and challenges and promote the safe, positive and constructive use of the internet.

2 Aims and Objectives

Durham School Dubai recognises that the internet is an essential part of modern education and provides valuable opportunities for learning, research, communication and collaboration. The school aims to provide safe, appropriate and purposeful access to technology while ensuring that pupils and staff understand how to use digital resources responsibly.

The aims of this policy are to:

- Provide safe and appropriate internet access that supports teaching and learning.
- Use effective filtering and monitoring systems to protect pupils from harmful or inappropriate content.
- Ensure filtering and monitoring arrangements are regularly reviewed and meet the school's safeguarding needs.
- Ensure clear roles and responsibilities are in place for managing online safety, filtering and monitoring.
- Educate pupils about responsible and safe internet use, including how to recognise and report inappropriate content.
- Develop pupils' ability to evaluate online information critically and recognise unreliable or inaccurate content.
- Protect personal information and ensure that login details are kept secure.
- Promote safe and appropriate use of email, websites, social media and digital communication.
- Ensure staff and pupils understand expectations around professional boundaries and online communication.
- Ensure the use of pupil photographs, work and personal information online is managed appropriately and with the necessary permissions.
- Ensure online safety concerns are reported, recorded and addressed promptly.

- Support pupils in developing the knowledge and skills needed to use technology safely, positively and responsibly.

The school will ensure that internet access is planned to enrich and extend learning, with access levels reviewed according to pupils' age, curriculum requirements and safeguarding needs.

3 Acceptable Use of Technology

3.1 Pupil Expectations

Pupils at Durham School Dubai are expected to use technology safely, responsibly and respectfully. Technology should support learning and should never be used to harm, intimidate or disrupt others.

Pupils must:

- Use school devices and networks for appropriate educational purposes.
- Follow instructions from staff when using technology.
- Keep usernames and passwords private and secure.
- Protect their own and others' personal information.
- Use respectful and appropriate language when communicating online.
- Only access websites, apps and content that are appropriate and permitted by the school.
- Tell a member of staff if they see or receive inappropriate, harmful or upsetting content.
- Treat emails, messages and online communication with the same respect as face-to-face communication.
- Check information found online and consider whether it is accurate and reliable.
- Respect copyright and acknowledge sources when using online material.
- Never share photographs, videos or personal information about another pupil without permission.
- Never attempt to bypass the school's filtering or security systems.
- Never use technology to bully, threaten, harass, impersonate or deliberately upset another person.
- Never arrange to meet someone they have met online without appropriate adult permission.
- Follow the school's Behaviour, Safeguarding and Anti-Bullying Policies when using technology.

If you are unsure whether something is appropriate, stop and ask a member of staff.

3.2 Staff Expectations

Staff are expected to model safe, professional and responsible use of technology at all times.

Staff must:

- Use school-approved devices, systems and email accounts where appropriate.
- Use a school landline phone when contact with parents or pupils is required.
- Keep personal phones in a bag or locker during the school day.
- Personal phones must not be used during teaching sessions. They may be used in the staffroom during break times.

- Never use a personal phone to take photographs, access the internet or communicate during teaching sessions.
- Keep passwords and login details secure and confidential.
- Never share personal contact details with pupils.
- Communicate with pupils only through school-approved systems.
- Maintain professional boundaries and never communicate with current pupils through personal social media.
- Protect confidential pupil, family and staff information.
- Ensure photographs, videos and pupil work are only shared through authorised school channels and with appropriate permission.
- Report any inappropriate, harmful or suspicious online content.
- Record and report online safety or safeguarding concerns through CPOMS and to the DSL where appropriate.
- Follow the school's Safeguarding, Behaviour, Anti-Bullying and Data Protection Policies.
- Personal devices and mobile phones are not to be used during lessons or other pupil contact times

3.3 Pupil Mobile Phones

Pupils are not permitted to use mobile phones during the school day. Where a pupil brings a mobile phone to school, with parental agreement, it must be handed to Reception at the start of the school day and collected after school. Further details are provided in the school's separate parent agreement regarding mobile phones.

4 Online Safety Rules for Staff

These rules help protect both staff and the school by setting clear expectations for the use of school computers, networks and internet services.

Staff must:

- Use the school network only through their authorised account and password. Passwords must never be shared.
- Use school ICT systems and internet access appropriately for educational and professional purposes.
- Respect copyright and intellectual property rights.
- Communicate professionally and politely, remembering that emails may be forwarded to unintended recipients.
- Never send anonymous messages or chain letters.
- Take care not to share personal or confidential information through email, messaging, blogs or other online platforms.
- Not use school ICT systems for personal purposes unless specifically authorised by the Head of School.
- Never use school systems for personal financial gain, gambling, political activity, advertising or illegal purposes.
- Report inappropriate or concerning online content or activity to the appropriate member of staff.
- Understand that inappropriate or irresponsible use may result in loss of network or internet access and may be subject to further action.

4.1 Monitoring and Security

The school reserves the right to monitor the use of its computer systems and network, including website access and email activity, where there is reason to believe that systems are being misused or used for unlawful or unauthorised purposes. This may include the interception of emails or removal of inappropriate or unlawful material.

Remember: School technology is provided for professional use. Use it responsibly, professionally and safely at all times.

5 Personal Devices

5.1 Mobile Phones

Staff

- Personal mobile phones must be kept in a bag or desk during the school day.
- Phones must not be used during teaching sessions, including for photographs, internet access or personal communication.
- Phones may be used in the staffroom during break times.
- When contacting pupils or parents, staff must use a school landline or approved school communication system.
- Staff must never use personal phones to take photographs or videos of pupils.

Pupils

- Mobile phones are not permitted for use during the school day.
- Where a pupil brings a phone to school with parental agreement, it must be handed to Reception at the start of the school day.
- Phones can be collected from Reception after school.
- Pupils must not use personal phones during lessons or on school premises during the school day.
- Any misuse will be managed in line with the Behaviour Policy.

The same expectations apply to personal smartwatches and tablets/iPads.

5.2 Smartwatches and Tablets

Staff

- Personal smartwatches and tablets should not be used during teaching sessions.
- Staff should not use personal devices to photograph or record pupils.
- Personal devices should not be used to access the internet or communicate with pupils during teaching time.
- Any communication with pupils or parents must use school-approved systems.

Pupils

- Smartwatches and tablets/iPads are not permitted for use during the school day.
- When brought to school with parental agreement, devices must be handed to Reception at the start of the school day.
- Devices can be collected after school.
- Pupils must not use devices to record, photograph, communicate with others or access the internet during the school day.

- Any misuse will be managed in line with the Behaviour Policy.

The same expectations apply to all personal electronic devices brought onto school premises.

5.3 Photography and Video

Staff

- Do not use personal mobile phones, tablets or other devices to photograph or record pupils.
- Photographs or videos should only be taken for authorised school purposes using school-approved equipment.
- Ensure any photographs or videos are stored and shared through approved school systems.
- Do not share pupil photographs or videos through personal social media, messaging apps or personal accounts.
- Follow the school's Safeguarding and Data Protection Policies when taking, storing or sharing images.
- Report any accidental or inappropriate recording of a pupil immediately to the appropriate member of the Safeguarding Team.

Pupils

- Pupils must not photograph or record other pupils or staff without permission.
- Images or videos must not be shared without appropriate consent.
- Pupils must never use images or recordings to bully, embarrass, threaten or humiliate another person.
- Any misuse of photography or video will be managed in line with the Behaviour and Anti-Bullying Policies.

If you are unsure whether you can take or share an image, do not do so - check with a member of the Senior Leadership Team first.

6 Social Media and Professional Boundaries

Staff must maintain clear professional boundaries when using social media and communicating online.

Staff Expectations

- Do not accept or add current pupils or parents on personal social media accounts.
- Do not communicate with pupils through personal social media, messaging apps or personal email.
- Do not share personal contact details with pupils.
- Do not promote personal social media accounts to pupils.
- Do not post, share or engage with content that could compromise your professional role or the reputation of the school.
- Do not discuss pupils, families or confidential school matters online.
- Use school-approved communication systems for contact with pupils and parents.
- Consider how online activity may be viewed by pupils, parents, colleagues and the wider community.

- Report any inappropriate online contact, messages or concerns to the DSL or appropriate member of the Safeguarding Team.
- Do not socialise with parents outside of school times or events.

Pupil Expectations

- Pupils should be encouraged to use social media responsibly and safely.
- Personal information, passwords and locations should not be shared online.
- Pupils should know how to block, report and seek help if they receive inappropriate or unwanted contact.
- Cyberbullying and inappropriate online behaviour will be addressed through the Anti-Bullying and Behaviour Policies.

Staff are adults in a position of trust; pupils are students, not friends.

7 Cyberbullying

Cyberbullying is bullying that takes place through digital technology, including social media, messaging apps, online games, email and other online platforms. It can have a significant impact on a pupil's wellbeing and safety.

Staff Expectations

- Take all reports of cyberbullying seriously.
- Listen to the pupil and reassure them that they have done the right thing by reporting it.
- Do not investigate independently or ask pupils to forward inappropriate content.
- Record the concern factually on CPOMS.
- Inform the Phase Leader or DSL where appropriate.
- Preserve relevant evidence, such as screenshots, where appropriate and safe to do so.
- Follow the Anti-Bullying, Behaviour and Safeguarding Policies.
- Continue to monitor the pupils involved and provide appropriate pastoral support.

Pupil Expectations

Pupils should:

- Report cyberbullying to a trusted adult.
- Not respond to threatening or abusive messages.
- Block and report users where appropriate.
- Never share, forward or encourage harmful content.
- Keep evidence where safe to do so.
- Remember that online behaviour can have real-world consequences.

If you have any concerns about cyberbullying or online behaviour, refer to the Anti-Bullying Policy and follow the school's reporting and recording procedures.

8 Online Child Protection Risks

8.1 Content

Content refers to what children may see, receive or access online.

This can include:

- Inappropriate or age-inappropriate material.
- Violent or graphic content.
- Sexual or exploitative content.
- Hate speech or discriminatory material.
- Extremist or radicalising content.
- Self-harm or harmful behaviour.
- Misinformation and misleading content.
- Inappropriate advertising or scams.
- AI-generated or manipulated content.

Staff should:

- Be aware of changes in a pupil's behaviour following online activity.
- Take concerns about online content seriously.
- Do not investigate or access inappropriate content unnecessarily.
- Record concerns on CPOMS and refer to the DSL where appropriate.
- Follow the Safeguarding and Child Protection Policy

8.2 Who to Contact

If you have a concern about online safety:

- Class Teacher / Form Tutor – for initial support and advice.
- Phase Leader / Head of School – for behaviour or ongoing concerns.
- Head of Pastoral – for pastoral or wellbeing concerns.
- Designated Safeguarding Lead (DSL) – for any safeguarding concern or risk of harm.
- IT Team – for technical issues, inappropriate websites or filtering concerns.

Always record concerns on CPOMS and inform the appropriate member of staff.

8.3 Conduct

Conduct refers to how children behave and interact online, and how their online behaviour may affect themselves or others.

Examples include:

- Cyberbullying or online harassment.
- Sharing hurtful, threatening or discriminatory messages.
- Sharing photographs, videos or personal information without permission.
- Impersonating or creating fake accounts.
- Sending or sharing inappropriate or harmful content.
- Pressure to send or share images.

- Online gaming behaviour, including inappropriate communication.
- Deliberately excluding or humiliating others online.
- Misuse of AI, including creating or sharing manipulated images.

Staff should:

- Take concerns seriously and listen without judgement.
- Record concerns factually on CPOMS.
- Refer safeguarding concerns to the DSL.
- Follow the Anti-Bullying, Behaviour and Safeguarding Policies.
- Continue to monitor and support pupils involved.

If online behaviour causes concern, report it; even if you are unsure whether it meets the definition of bullying.

8.4 Commerce

Commerce refers to the financial risks children may face when using the internet, including:

- Online scams and fraud.
- In-app or online purchases.
- Pressure to buy products or services.
- Gambling or gambling-like activities.
- Sharing bank or payment details.
- Phishing emails, messages or fake websites.
- Identity theft or misuse of personal information.
- Online games or apps encourage spending.
- Paid adult websites.

Staff should:

- Encourage pupils to never share financial or personal information online.
- Be alert to concerns about money, online purchases or suspicious messages.
- Record concerns on CPOMS.
- Refer safeguarding concerns to the DSL.
- Report technical or suspicious website concerns to the IT Team.
- Artificial Intelligence (AI)

8.5 AI

AI can be a useful learning tool, but it also presents risks for children, including:

- Sharing personal or confidential information with AI tools.
- Creating or sharing fake or manipulated images and videos.
- Using AI to create harmful, threatening or discriminatory content.
- AI-generated bullying or harassment.
- Exposure to inappropriate or harmful AI-generated content.
- Relying on AI-generated information that may be inaccurate or misleading.
- Using AI to impersonate or deceive others.

Staff should:

- Follow the school's guidance on the appropriate use of AI.
- Remind pupils not to share personal information with AI tools.
- Take concerns about AI-generated content seriously.
- Record concerns on CPOMS.
- Refer safeguarding concerns to the DSL.
- Report technical concerns to the IT Team.

If AI is being used to harm, threaten, bully or exploit a pupil, report it immediately.

9 Responding to Online Safety Concerns

If you are concerned about a pupil's online safety:

- Listen and reassure the pupil.
- Do not investigate or ask leading questions.
- Record the concern on CPOMS as soon as possible.
- Inform the DSL immediately if there is a safeguarding concern.
- Report technical concerns, such as inappropriate websites or filtering issues, to the IT Team.
- Preserve relevant evidence where appropriate, but do not forward or share inappropriate content.
- Follow the Safeguarding, Anti-Bullying and Behaviour Policies.
- Continue to monitor and support the pupil.

Remember: Recognise → Respond → Record → Refer

10 Filtering and Monitoring

Durham School Dubai uses filtering and monitoring systems to help protect pupils from harmful or inappropriate online content while supporting safe and purposeful internet use.

10.1 Authorising Internet Access

- Pupils will be taught about acceptable internet use.
- All staff must read and sign the Staff Information Systems Code of Conduct before using school ICT resources.
- The IT Technician will maintain a current record of staff and pupils with access to school ICT systems.
- Access records will be available to the Online Safety Coordinator.

10.2 Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material.
- Due to the nature and size of the internet, it is not possible to guarantee that unsuitable material will never appear.

- Staff and pupils should report inappropriate content or websites immediately.
- The school cannot accept liability for material accessed or the consequences of internet access.

10.3 Online Safety Complaints

- Complaints about internet misuse will be dealt with by the Head of School.
- Complaints regarding staff misuse must be referred to the Head of School.
- Concerns relating to child protection must be managed in accordance with the Safeguarding and Child Protection Policy.
- Pupils and parents will be informed of the complaints procedure where appropriate.

Filtering and monitoring support safeguarding, but all staff remain responsible for reporting concerns and promoting safe internet use.

11 Data Protection, Privacy and Confidentiality

Durham School Dubai is committed to protecting the personal information and privacy of pupils, staff and families.

Staff must:

- Keep personal and confidential information secure.
- Only access information that is necessary for their role.
- Never share pupil or family information with unauthorised people.
- Use school-approved systems when storing or sharing information.
- Never share passwords or login details.
- Take care when sending emails, particularly when they contain confidential information.
- Never discuss pupils, families or safeguarding concerns in public or on social media.
- Ensure photographs and videos of pupils are only taken, stored and shared through approved school systems and with appropriate permission.
- Follow the school's Data Protection Policy when handling personal information.
- Report any suspected data breach or accidental disclosure to the appropriate member of staff immediately.
- Use online and IT assets in-line with the School's Data Protection Policy.

11.1 Confidentiality and Safeguarding

Safeguarding concerns must be treated confidentially. Staff should only share information with those who need to know in order to safeguard a child.

Never promise a pupil confidentiality. Explain that information may need to be shared with the appropriate safeguarding staff if someone is at risk of harm.

Protect information. Protect pupils. Share information only when necessary and appropriate.

11.2 Communications

Introducing the Policy to Pupils

- Pupils will be taught age-appropriate acceptable use of technology.
- Pupils will be informed that network and internet use is monitored.

Staff and the Policy

- All staff will receive the Online Safety Policy and its importance will be explained.
- Staff should understand that internet activity can be monitored and traced to individual users.
- Staff must maintain professional conduct and discretion when using school systems.
- Filtering and monitoring will be overseen by Senior Management, with clear procedures for reporting concerns or issues.

12 Parents' Support

Parents play an important role in keeping children safe online. Online safety is a shared responsibility between school and home, and parents need to understand the risks children may face and how they can support safe and responsible use of technology.

Durham School Dubai will:

- Make parents aware of the Online Safety Policy through regular school communications.
- Provide online safety workshops for Primary and Secondary parents.
- Share guidance and key online safety messages through newsletters.
- Use the school website and social media to share relevant advice, updates and resources.
- Encourage parents to talk openly with their children about their online experiences and know where to seek help if they have concerns.
- Work in partnership with parents to promote safe, responsible and age-appropriate use of technology at home.

13 Online Safety Incidents: Recording and Reporting

- All online safety concerns must be taken seriously and reported.
- Staff should record concerns on CPOMS as soon as possible.
- Record factual information, including what was seen, heard or disclosed.
- Do not investigate the concern yourself or make assumptions.
- Safeguarding concerns must be reported directly to the DSL.
- Cyberbullying concerns should also be managed in line with the Anti-Bullying Policy.
- Technical concerns, such as inappropriate websites or filtering issues, should be reported to the IT Team.
- Relevant evidence, such as screenshots, should be preserved where appropriate.
- Continue to monitor and support the pupil following a concern.
- CPOMS records should be reviewed regularly to identify patterns or repeated concerns.

14 Parents and Carers

Parents and carers play an important role in supporting children to stay safe online. Durham School Dubai encourages open communication between home and school.

Parents and carers should:

- Talk regularly with their child about their online experiences.
- Encourage children to speak to a trusted adult if something online makes them feel worried, uncomfortable or unsafe.
- Set age-appropriate boundaries around devices, apps, games and social media.
- Be aware of the apps and platforms their child uses.
- Encourage children to protect personal information and use strong passwords.
- Know how to block and report inappropriate online behaviour.
- Monitor online activity appropriately, while maintaining open and supportive communication.
- Report any online safety concerns to the School.
- Attend school online safety workshops and engage with guidance shared through newsletters, the website and social media.

School and home working together helps children develop safe, responsible and positive online habits.

15 Policy Information

Policy Title: Online Safety Policy

Policy Owner: Designated Safeguarding Lead

Approved By: Principal and Chair of the Board of Governors

Applies To: All staff, governors, volunteers, contractors, visitors and third-party providers

Review Frequency: Annually (or sooner if required)

Next Review Date: August 2027

Approved by



Oliver Bromley Hall
Principal



Saumya Basu
Chair of the Board of Governors

Change History Record

Version No.	Description of Change	Owner	Date of Issue
1.0	Policy Written	Principal	September 2023
2.0	Updates	Principal	August 2026

Durham School Dubai's Policies and Guidelines

Durham School Dubai policies have been developed by the School Leadership Team (SLT) with input and guidance from a network of Dubai schools, including Durham School UK.

Policies reflect current best practice. At the time of writing, policies aligned with the following: