

PROCEDURE E-SAFETY (DIGITAL AND ONLINE)	Owner	E-Safety (Digital and Online) Leads
	ID (Version)	DU/5.1.1.3 (v3)
	Published	15 August 2024
	Valid Until	15- August 2025 (Annual)

INTRODUCTION

1. PURPOSE / SCOPE

The Arbor School (“Arbor,” “we,” “the school”) is committed to ensuring that all staff are responsible for digital safety including the acceptable use of digital networks, hardware, and software to protect employees and students at The Arbor School.

Digital safety encompasses internet technologies and electronic communications such as iPads as well as collaboration tools and electronic publishing. It highlights the need to educate students and staff about the benefits and risks of using technology and provides protection and awareness for users to enable them to make safe and responsible decisions to control their online experiences.

At the Arbor School (“Arbor”, “we”, “the school”), we understand the importance of effective digital safety practices for students and staff, and this policy sets out how we ensure this is achieved.

2. RELATED DOCUMENTS

This policy should be read and applied in conjunction with all relevant governance documents within the school and related reference documents, whether existing or introduced and / or modified subsequent to this procedure being published, including (but not limited to):

Document Title	ID / Reference No.
Students	
Safeguarding and Child Protection Policy	DU/5.1.1
Child-on-Child Abuse Procedure	DU/5.1.1.2
Student Acceptable User Policy	Appendix A
Staff	
Managing Allegations Against Staff Policy	DU/5.2.1
Managing Allegations Against Staff Procedure	DU/5.2.1.1
Social Media Procedure	DU/5.1.1.12
Staff Acceptable User Policy	Appendix A
Health and Safety	
School Trip Volunteer Declaration	
Information Management Policy	DU/1.2.3

3. RESPONSIBILITY ASSIGNMENT

The following position(s) / role(s) has / have been assigned the responsibilities hereunder in relation to the execution of the guidelines, requiring the relevant responsible individual(s) to ensure that they are communicated to, understood, and adhered to by all applicable school employees:

Responsibility	Position(s) / Role(s)
Responsible	Teachers and Learning Support Assistants
Accountable	Senior IT manager and Digital Safeguarding Leads
Consulted	Designated Safeguarding Lead and Governing Body
Informed	Parents/Community

PROCEDURE E-SAFETY (DIGITAL AND ONLINE)	Owner	E-Safety (Digital and Online) Leads
	ID (Version)	DU/5.1.1.3 (v3)
	Published	15 August 2024
	Valid Until	15- August 2025 (Annual)

GUIDELINES

4. DEFINITIONS OF RISK

What are the four categories of risk?

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: 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:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images (e.g., consensual, and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images, upskirting, and online bullying.
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing.

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for students. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.

5. DEVICE ACCESS WITHIN THE SCHOOL DAY

Screens will be used for educational purposes only in alignment with the UK National Curriculum. Recreational or non-educational screen time is generally not permitted during school hours.

- **Age-Appropriate Content:** All digital content used must be age-appropriate and relevant to the curriculum, or suitable for leisure viewing during designated times.
- **Teacher Supervision:** Screen time must be supervised by a teacher to ensure that it is being used appropriately and effectively.
- **Balanced Schedule:** Screen time will be integrated into a balanced schedule that includes a variety of learning activities, including physical activity, hands-on learning, and face-to-face interaction.
- **Break and Lunch Screen Time:** During particularly hot weather, screens may be used to show age-appropriate audio-visual stories only. Films and programmes are not permitted. Adverts should be minimised using chrome extensions (ad blockers) and Safetube links.
- **Break and Lunch iPad Use:** iPad are not permitted during breaktimes or lunchtimes.
- **Film Viewing:** Films or videos are not suitable for lunchtime, playtime or end of day dismissal. When a film or video is viewed, it must be pre-approved by the year group leader and suitable for the students' age group. This is an exception and should not become a regular practice. It is reserved for exceptional circumstances and aligns with the curriculum.

PROCEDURE	Owner	E-Safety (Digital and Online) Leads
E-SAFETY (DIGITAL AND ONLINE)	ID (Version)	DU/5.1.1.3 (v3)
	Published	15 August 2024
	Valid Until	15- August 2025 (Annual)

Year Group	Usage Type	Access
FS1	Primarily for interactive educational games and basic computer skills.	Lessons: iPads may be used during small group activities each week to enhance learning. Screens may be used during whole class activities or during exploration time. Regular breaks will be scheduled to minimize eye strain and encourage physical activity. Location: Screens will be used in the classroom under direct teacher supervision.
FS2		
Year 1	Primarily for interactive educational software, research skills, and multimedia applications including Seesaw.	Lessons: Computing is taught once per week however iPads may be used to enhance learning during a variety of lessons within a week. Screens may be used during whole class activities. Regular breaks will be scheduled to minimize eye strain and encourage physical activity. Location: Screens will be used in the classroom under direct teacher supervision.
Year 2		
Year 3		
Year 4		
Year 5	Research projects, educational activities, and multimedia content creation including Canva, Seesaw and Office 365.	Lessons: Computing is taught once per week; however, iPads are available on a 1:1 basis and may be used daily during a variety of lessons to enhance learning. Regular breaks will be scheduled to minimize eye strain and encourage physical activity. Location: Classroom and specialist lessons under direct teacher supervision through Apple Classroom.
Year 6		

6a. MANGEMENT OF INTERNET ACCESS

The IT department will use a range of firewalls, filters, and processes to maintain safe internet access for staff and students on all digital devices within The Arbor School.

- The security of the school’s information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school uses effective firewalls and filters and ensures that users cannot remove filters for illegal content including VPNs.
- The filtering system can enforce the use of ‘safe search’ functionality.
- Internet history is regularly exported and reviewed.
- Access to websites identified as inappropriate is removed and logged.
- Bandwidth heavy resources such a video and audio streaming should be removed to maintain quality of service for all.
- The school will work in partnership with the service provider to ensure filtering systems are as effective as possible.
- Senior staff will ensure that checks are made to ensure that the filtering methods selected are appropriate, effective, and reasonable. When checks are made, the IT team are notified prior, and accompanied by another member of staff. These risk assessments are logged.

PROCEDURE	Owner	E-Safety (Digital and Online) Leads
E-SAFETY (DIGITAL AND ONLINE)	ID (Version)	DU/5.1.1.3 (v3)
	Published	15 August 2024
	Valid Until	15- August 2025 (Annual)

- Emerging technologies will be examined for educational benefit and a trial will be carried out by Designated Digital Safeguarding Leads.
- Parents, staff, and students will be asked to sign and return a consent form agreeing to comply with the school's *Acceptable Use Guidelines* ([appendix A](#)).

6b. INTERNET ACCESS FOR STUDENTS

The school internet access is designed expressly for student use and includes filtering appropriate to the age of the students however vulnerability and risk of harm is also considered.

- Students will be taught what internet use is acceptable and what is not and will be given clear objectives for Internet use that are specific, measurable, achievable, relevant, and timely (“SMART”).
- Internet access will be for educational purposes only and planned to enrich and extend learning activities.
- Students will receive an Acceptable Use Policy (AUP) at the start of every year ([appendix A](#)).
- Staff will guide students in online activities that will support the learning outcomes planned for the students’ age and maturity and educate them in the effective use of the internet in research, including the skills of knowledge location, retrieval, and evaluation. Staff will actively monitor all screen activity during a lesson either physically or from a central console using appropriate technology.

Year Group	Access Type	Comments
FS1	Shared devices	Only pre-approved websites are available to students via QR codes. Students are directly supervised when using devices.
FS2		
Year 1	Shared devices	Key Stage 1 Only pre-approved websites are available to students via QR codes. Students are directly supervised when using devices. Students are taught how to use child safe search engines within Computing including Swiggle, Kiddle, Safe Search Kids
Year 2		
Year 3		
Year 4		
Year 5		
Year 6	Individual accounts (1:1 iPads)	Upper Key Stage 2 Students are directed when to use their devices. Most websites are pre-approved however where appropriate, child friendly search engines will be used strategically, and students will evaluate the digital content critically to determine its relevance and reliability in line with the national curriculum. Apple classroom will be used to monitor devices in Year 5 and 6 due to the 1:1 devices being used.
Year 7	Individual accounts	

PROCEDURE	Owner	E-Safety (Digital and Online) Leads
E-SAFETY (DIGITAL AND ONLINE)	ID (Version)	DU/5.1.1.3 (v3)
	Published	15 August 2024
	Valid Until	15- August 2025 (Annual)

Year 8		Students have filtered access to the internet appropriate for their key stage.
Year 9		Students have access to search engines using enforced safe search options.
Year 10	Individual accounts	Students have filtered access to the internet appropriate for their key stage.
Year 11		Students have access to search engines using enforced safe search options.
Year 12 Year 13	Individual accounts	Students have filtered access to the internet appropriate for their key stage. Students have access to search engines using enforced safe search options.

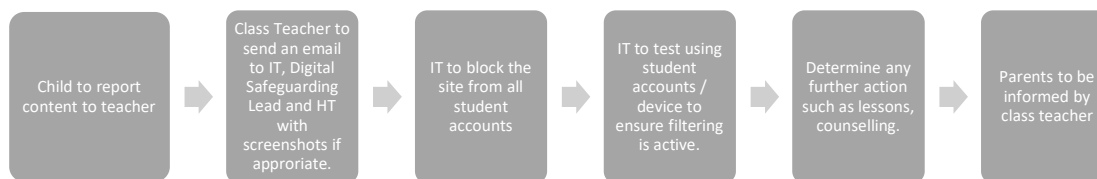
How are students introduced to Internet Safety?

- Student Acceptable Use Policies will be shared with all KS1 and KS2 students.
- Student Acceptable Use Policies will be posted in all networked rooms and on device trolleys.
- Students will be informed that internet use will be monitored.
- Advice on e-safety will be shared throughout the academic year to raise awareness and the importance of safe and responsible internet use in line with the Computing curriculum.
- Students will receive lessons on digital safety which aligns with our Digital Safety curriculum ([appendix B](#)).

7. REPORTING UNSUITABLE CONTENT

It is important that any changes to the filter system are logged enabling an audit trail as well as transparency.

- If students or staff discover unsuitable sites, the uniform resource locator (“URL”) address, date and content must be reported via email to the school’s IT Team, Digital Safeguarding Lead, and the Head Teacher.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students will be taught what to do if they find inappropriate content online that makes them feel uncomfortable using the following flow diagram.



8. PROTECTING PERSONAL DATA

- Personal data will be recorded, processed, transferred, and made available according to the school’s *Information Management Policy*.
- All access to personal data will be password-protected.
- A data protection impact assessment will be implemented yearly.

9. EMAIL

- Students and Staff may only use approved e-mail accounts, via the Microsoft Office 365 Platform.

PROCEDURE E-SAFETY (DIGITAL AND ONLINE)	Owner	E-Safety (Digital and Online) Leads
	ID (Version)	DU/5.1.1.3 (v3)
	Published	15 August 2024
	Valid Until	15- August 2025 (Annual)

- Students and Staff are not allowed access to personal e-mail accounts whilst in school.
- Students and Staff must immediately inform an adult if they receive an offensive e-mail.
- Students and Staff must immediately inform IT if they receive a phishing e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.

10. PUBLISHED CONTENT

Publications sent to an external organization should be authorized by the marketing team before. All published material should be written carefully and proofread. Publications include written material as well as video and photographic footage.

- Photographs that include students will be used on the school’s website or on social media thoughtfully, and only with parental permission. All publications on Arbor social media must abide by the *Social Media Procedure*.
- Students’ full names will not be used anywhere on the website or in publications, particularly in association with photographs unless preapproved by the marketing team and parental consent is provided.
- If the student’s face is in the photograph for a social media post, then their name should not be included.
- School trip volunteers will not use personal devices to take photos or film the students, including their own child as per the safeguarding declaration for school trips.

11. MANAGING VIDEOCONFERENCING

- Internet Protocol (“IP”) videoconferencing should use Microsoft Office 365 as the preferred option to ensure quality of service and security. Zoom may be used as an alternative.
- Students should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing should be supervised appropriately.
- Microsoft Teams should only be used within school hours.
- Remote lessons should be recorded.

12. PERSONAL DEVICES FOR STUDENTS

The safe and acceptable use of devices and the internet outside of school hours is the responsibility of parents / carers, who are recommended to ensure:

- Devices are used in supervised, shared, communal areas within the house and discourage the use of devices in bedrooms.
- Set time limits on devices and turn off notification settings.
- Set up family linked devices.
- Check settings to ensure that highest privacy settings are activated, deactivate chat functions and geolocation settings.
- Check the PEGI ratings of APPs to ensure only APPs of a suitable age are used.
- Report any inappropriate content to the provider.
- Discuss digital footprint.
- Be alert to children becoming upset or secretive, or changing relationships with friends, after using the internet / devices.
- Be aware that a child may be as likely to be a bully as to be a target.
- Start discussions with their children and understand how they are using the internet / devices.

PROCEDURE	Owner	E-Safety (Digital and Online) Leads
E-SAFETY (DIGITAL AND ONLINE)	ID (Version)	DU/5.1.1.3 (v3)
	Published	15 August 2024
	Valid Until	15- August 2025 (Annual)

- Remind their children of the UAE law regarding defamation of character, sharing photographs and private information without consent as well as using offensive or defamatory language.

The school will be proactive and sensitive to internet-related issues experienced by students out of school and will:

- Teach Digital Safety Lessons including how to remain safe when using their own devices.
- Be proactive in reminding the community about UAE laws regarding defamation of character, sharing photographs without consent, disclosing private information, using offensive language.
- Respond effectively to reports of cyber-bullying or harassment and will abide by the *Child-on-Child Abuse Procedure* and *Safeguarding and Child Protection Policy/Protection*.
- Encourage pupils to Speak Out and Stay Safe through self-reporting QR codes and termly surveys. The national reporting app "Hemayati" is available on all iPads. Where 1:1 devices are available, pupils will also have access to wellbeing applications such as You Hue.
- Limit use of personal devices during the school day including on school transport.

The school will be proactive and sensitive to internet-related issues experienced by parents and will:

- Draw parents and carers attention to the *Digital Policy* through newsletters, email, social media and on the website.
- Contact parents where concerns have been raised about a student's access to age-inappropriate games, films, and online media etc.
- Invite parents to attend workshops to support the use of technology at home and to raise awareness of digital risks.

13. HANDLING DIGITAL SAFETY COMPLAINTS

Complaints against staff will be dealt with in accordance with the school's *Managing Allegations Against Staff Policy and Procedure*.

Complaints of a child protection nature must be dealt with in accordance with the school's *Safeguarding and Child Protection Policy and Procedure*.

Complaints of Cyberbullying will abide by the school's *Child-on-Child Abuse Procedure*. Cybercrimes committed will be reported to the Dubai Police by the DSL ([appendix C](#)).

In terms of internet misuse, [Arbor](#)haviour steps will be followed.

PROCEDURE	Owner	E-Safety (Digital and Online) Leads
E-SAFETY (DIGITAL AND ONLINE)	ID (Version)	DU/5.1.1.3 (v3)
	Published	15 August 2024
	Valid Until	15- August 2025 (Annual)



Steps	Possible actions
1) Reminder	A reminder of the rules Ready, Respectful, Safe delivered privately wherever possible, making the word 'reminder' explicit to them and the next steps if their behaviour does not improve; show disappointment, emphasise student choices, deescalate where possible and take the initiative to keep things at this stage. Teachers may need to give reminders to stay on task.
2) Reflection (Teacher)	Give the learner a chance to reflect away from others and break or lunchtimes may be used if appropriate, a 'Reflection Time' sheet must be completed. Speak to the learner privately and give them a final opportunity to engage. Offer a positive choice to do so.
3) Reflection (Head of Year)	At this point, the learner will be referred internally to the Head of Year, they must take their initial Reflection Time form with them to show the Head of Year.
4) Internal referral (Senior Leadership)	At this stage, the learner will be referred to the Assistant Head Student Welfare and Support Services, who will decide the appropriate course of action. Parents will be informed, and incidents logged on Nexquare.

However, in extreme cases where devices are used inappropriately, examples include but are not limited to vandalism, inappropriate language, fighting, bullying, stealing or hateful language it will be expedited to Step 4: Internal referral.

Internal referrals will be dealt with by a senior member of staff. Consequences may include reflection, interview/counselling by the Teacher / Principal, informing parents or carers, and removal of the internet or computer access for a period of time.

Students who are victims of cyberbullying are encouraged to not respond, tell a trusted adult and to show the offensive material to a trusted adult. Students are also encouraged to block and report their profile. Offensive material must only be communicated to the DSL, Principal, or DDSL ([appendix C](#)). In cases where illegal content is involved, members of staff should not copy, share or print the content.

PROCEDURE	Owner	E-Safety (Digital and Online) Leads
E-SAFETY (DIGITAL AND ONLINE)	ID (Version)	DU/5.1.1.3 (v3)
	Published	15 August 2024
	Valid Until	15- August 2025 (Annual)


Where appropriate, staff may ask to see school devices and **PERSONAL** devices may be confiscated within the school premises. The DSL or DDSL may check the device if that child or another child is deemed to be at harm. Any images or digitally shared materials must not be viewed, saved, shared, or printed by anyone other than the DSL, Principal, or DDSL ([appendix C](#)).

ABBREVIATIONS AND DEFINITIONS

Abbreviation / Term	Description / Definition
KCSIE	Keeping Children Safe in Education
SLT	Senior Leadership Team
DSL	Designated Safeguarding Lead
DSP	Designated Senior Person
DDSP	Deputy Designated Senior Person
DSG	Designated Safeguarding Governor
CPOMS	Child Protection Online Management System
UAE	United Arab Emirates
AUP	Acceptable Use Policy
URL	Uniform Resource Locator
IT	Information Technology
VPN	Virtual Private Network

PROCEDURE E-SAFETY (DIGITAL AND ONLINE)	Owner	E-Safety (Digital and Online) Leads
	ID (Version)	DU/5.1.1.3 (v3)
	Published	15 August 2024
	Valid Until	15- August 2025 (Annual)

AUTHORISATION HISTORY

Authority	Signature	Date
Designated Safeguarding Lead		15/08/2024
Principal		
Director of Education		

PROCEDURE	Owner	E-Safety (Digital and Online) Leads
E-SAFETY (DIGITAL AND ONLINE)	ID (Version)	DU/5.1.1.3 (v3)
	Published	15 August 2024
	Valid Until	15- August 2025 (Annual)

APPENDICES

APPENDIX A: ACCEPTABLE USE POLICIES

PROCEDURE	Owner	E-Safety (Digital and Online) Leads
E-SAFETY (DIGITAL AND ONLINE)	ID (Version)	DU/5.1.1.3 (v3)
	Published	15 August 2024
	Valid Until	15- August 2025 (Annual)

THE ARBOR SCHOOL

STAFF AGREEMENT

OUR PLEDGE TO KEEP STUDENTS SAFE

- Use safe search engines if applicable such as *youtubekids* and *Safesearchkids, Kiddle and Swiggle* when directing students
- Direct to prepared websites using QR codes to support safe searching when possible
- Closely monitor iPads when in use
- Use Apple Classroom for monitoring in Upper Key Stage Two
- iPads to be used for educational purposes only in class
- iPads to be returned to the trolley and locked daily.
- Only use school devices for photographing students
- If staff or students discover unsuitable sites, the uniform resource locator ("URL") address, date and content must be reported to the head teacher and Helpdesk.
- Students should be taught digital safety in line with the Computing Curriculum
- Student's names should not be used alongside photos on Social Media
- Remote lessons should be recorded
- Use school devices for work purposes only
- Do not make copies of any illegal offensive material including printing, sharing or copying, instead show it via the original device to the DSL, DDSL



PROCEDURE	Owner	E-Safety (Digital and Online) Leads
E-SAFETY (DIGITAL AND ONLINE)	ID (Version)	DU/5.1.1.3 (v3)
	Published	15 August 2024
	Valid Until	15- August 2025 (Annual)

THE ARBOR SCHOOL

STUDENT AGREEMENT

OUR PLEDGE TO BE CONFIDENT AND SAFE USERS IN THE ONLINE WORLD

- I will use school devices for educational purposes only at home and at school
- I will responsibly protect my personal information
- I will use Teams for educational purposes only. I will use Teams in school hours and only as directed by the class teacher.
- I will spread positivity, respect and kindness online
- When in doubt, talk it out. I will be an upstander and not a bystander. I will tell my teacher if there is any inappropriate behaviour or content.
- I will access age appropriate content
- I will only use applications directed by the school on my device.
- I will thoughtfully share with care. If it isn't right to say, it isn't right to post.



PROCEDURE	Owner	E-Safety (Digital and Online) Leads
E-SAFETY (DIGITAL AND ONLINE)	ID (Version)	DU/5.1.1.3 (v3)
	Published	15 August 2024
	Valid Until	15- August 2025 (Annual)

iPad

General Precautions

1. The iPad is the school's property and should be treated with respect and care.
2. The iPads come in an approved heavy duty hard casing, which offers protection.
3. iPads must always be within the protective case.
4. Cords/cables must be installed carefully into the iPad to prevent damage.
5. Students are responsible for keeping their iPad protected in the correct charging trolley for each school day.
6. Students will be using their iPads inside the school.
7. Students will use computer/devices in a responsible and ethical manner.
8. Students will use the Internet in a safe and appropriate manner and any offensive or inappropriate websites must be reported to a class teacher immediately so that they can be blocked.

Responsibilities

1. If a student accidentally or deliberately drops or damage their own device they are completely responsible for the damages, replacement, and repair.
2. If a student accidentally or deliberately drops or damage another student device they are completely responsible for the damages, replacement, and repair.
3. Arbor management will investigate and collect the information related to any damage case, the incident report will be shared with the parent for them to discuss and/or submit an appeal.
4. Parents will be informed that the School will send the broken device for repair at an Authorized Apple Service Provider and the finance department will invoice the student/s who are at fault

6. I accept the Acceptable User Policy for the use of a iPad

Yes

No

PROCEDURE	Owner	E-Safety (Digital and Online) Leads
E-SAFETY (DIGITAL AND ONLINE)	ID (Version)	DU/5.1.1.3 (v3)
	Published	15 August 2024
	Valid Until	15- August 2025 (Annual)

Surface Pro

1. I understand that this device is provided free of charge for the duration of my education at The Arbor School.
2. I understand that the if I decide to leave The Arbor School before the completion of Year 13 I must return the device to The School.
3. I understand that I am fully responsible for the maintenance of the device and I will bare all costs involved to ensure it is in a fully working condition until the above mentioned date.
4. If the device is beyond repair I will replace the device with a equal or higher specification device
5. I understand that use of the device in school is managed by The Arbor School's Mobile Device Management System.
6. I understand that the standard school filtering system will be applied to all internet traffic and I will not attempt to bypass this.
7. It is my responsibility to ensure the device is full charged each day and I understand that charging in school is not guaranteed.
8. I must not use the personal profile when in school and any use of the profile will result in sanctions
9. I understand the school has the right to amend this policy at its own discretion.

7. I accept the Acceptable User Policy for the use of a Surface Pro

Yes

No

PROCEDURE	Owner	E-Safety (Digital and Online) Leads
E-SAFETY (DIGITAL AND ONLINE)	ID (Version)	DU/5.1.1.3 (v3)
	Published	15 August 2024
	Valid Until	15- August 2025 (Annual)

School Devices

1. I understand that the schools will monitor my use of the systems, devices and digital communications.
2. I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person’s username and password.
3. I understand that the school’s systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
4. I will respect others’ work and property and will not access, copy, remove or otherwise alter any other user’s files, without the owner’s knowledge and permission.
5. I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
6. I will not take or distribute images of anyone without their permission.
7. I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information).
8. I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

4. I accept the above Acceptable User Policy *

- Yes
- No

PROCEDURE E-SAFETY (DIGITAL AND ONLINE)	Owner	E-Safety (Digital and Online) Leads
	ID (Version)	DU/5.1.1.3 (v3)
	Published	15 August 2024
	Valid Until	15- August 2025 (Annual)

APPENDIX B: DIGITAL CURRICULUM OVERVIEW

Year 1	Year 2	Year 3	Year 4	Year 5	Year 6
<p>Term 1.1 Online Relationships I can give examples of when I should ask permission to do something online and explain why this is important. I can use the internet with adult support to communicate with people I know (e.g., video call apps or services) I can explain why it is important to be considerate and kind to people online and respect their choices.</p>	<p>Term 1.1 Online Relationships I can give examples of how someone might use technology to communicate with others they don't also know offline and explain why this might be risky. I can describe different ways to ask for, give or deny my permission online and can identify who to help me if I am not sure. I can explain why I have a right to say 'no' or 'I will have to ask someone'. I can identify who can help me if something happens online without my consent. I can explain how it may make others feel if I do not ask their permission or ignore their answers before sharing something about them online. I can explain why I should always ask a trusted adult before clicking 'yes', 'agree', or 'accept' online</p>	<p>Term 1.1 Online Relationships I can describe ways people who have similar likes and interests can get together online. I can explain what it means to 'know someone' online and why this might be different from knowing someone offline. I can explain what is meant by 'trusting someone' online, why this is different to 'liking someone' online, and why it is important to be careful about who to trust online including what information and content they are trusted with. I can explain why someone may change their mind about trusting anyone with something if they feel nervous, uncomfortable or worried. I can explain how someone's feelings can be hurt by what is said or written online. I can explain the importance of giving and gaining permission before sharing things online; how the principles of sharing online is the same as sharing offline e.g. sharing images and photos</p>	<p>Term 1.1 Online Relationships I can describe strategies for safe and fun experiences in a range of online social environments e.g., livestreaming, gaming platforms. I can give examples of how to be respectful to others online and how to recognise healthy and unhealthy behaviours. I can explain how content shared online may feel important to one person but may be important to other people's thoughts, feelings and beliefs.</p>	<p>Term 1.1 Online Relationships I can describe forms of technology – specific forms of communication (e.g., emojis, memes, gifs) I can explain that there are some people I can communicate with online who may want to do me or my friends harm/ I can recognise this is not my/our fault. I can describe some of the ways people may be involved in online communities and describe how they might collaborate constructively with others and make positive contributions. (e.g., gaming communities or social media groups) I can explain how someone can get help if they are having problems and identify when to tell a trusted adult. I can demonstrate how to support others (including those who are having difficulties) online.</p>	<p>Term 1.1 Online Relationships I can explain how sharing something online may have an impact positively or negatively. I can describe how to be kind and show respect for others online including the importance of respecting boundaries regarding what is shared about them online and how to support them if others do not. I can describe how things shared privately online can have unintended consequences for others. E.g., Screenshots I can explain that taking or sharing inappropriate images of someone (e.g. embarrassing images), even if they say it is okay, may have an impact for the sharer and others; and who can help if someone is worried about this.</p>
<p>Term 1.1 Privacy and Security I can explain that passwords are used to protect information, accounts and devices I can recognise more detailed examples of information that is personal to someone (e.g., where someone lives and goes to school, family names) I can explain why it is important to always ask a trusted adult before sharing any personal information online, belonging to myself or others.</p>	<p>Term 1.1 Privacy and Security I can explain how passwords can be used to protect information, accounts and devices. I can explain and give examples of what is meant by 'private' and 'keeping things private' I can describe and explain some rules for keeping personal information private (e.g. creating and protecting passwords) I can explain how some people may have devices in their homes connected to the internet and give some examples (e.g. lights, fridges, toys, televisions.)</p>	<p>Term 1.1 Privacy and Security I can describe simple strategies for creating and keeping passwords private. I can give reasons why someone should only share information with people they choose to and can trust. I can explain that if they are not sure of feel pressured then they should tell a trusted adult. I can describe how connected devices can collect and share anyone's information with others.</p>	<p>Term 1.1 Privacy and Security I can describe strategies for keeping personal information private, depending on context. I can explain that internet use is never fully private and is monitored e.g. adult supervision I can describe how some online services may seek consent to store information about me; I know how to respond appropriately and who I can ask if I am not sure. I know what the digital age of consent is and the impact this has on online services asking for consent.</p>	<p>Term 1.1 Privacy and Security I can explain what a strong password is and demonstrate how to create one. I can explain how many free apps or services may read and share private information (e.g., friends, contacts, likes, images, videos, voice messages, geolocation) with others. I can explain what app permissions are and can give some examples</p>	<p>Term 1.1 Privacy and Security I can describe effective ways people can manage passwords (e.g. storing them securely or saving them in the browser). I can explain what to do if a password is shared, lost or stolen. I can describe how and why people should keep their software and apps up to date e.g. auto updates. I can describe simple ways to increase privacy on apps and services that provide privacy settings. I can describe ways in which some online content targets people to gain money or information illegally; I can describe strategies to help me identify such content (e.g. scams, phishing) I know that online services have terms and conditions that govern their use.</p>
<p>Term 1.1 Health and Wellbeing I can explain rules to keep myself safe when using technology both in and beyond the home</p>	<p>Term 1.1 Health and Wellbeing I can explain simple guidance for using technology in different environments and settings e.g., accessing online technologies in public places and the home environment. I can say how those rules/guides can help anyone accessing online technologies</p>	<p>Term 1.1 Health and Wellbeing I can explain why spending too much time using technology can sometimes have a negative impact on anyone, e.g. mood, sleep, body, relationships; I can give examples of both positive and negative activities where it is easy to spend a lot of time engaged (e.g. doing homework, games, films, videos) I can explain why some online activities have age restrictions, why it is important to follow them and know who I can talk to if others pressure me to watch or do something online that makes me feel uncomfortable</p>	<p>Term 1.1 Health and Wellbeing I can explain how using technology can be a distraction from other things, in both a positive and negative way. I can identify times or situations when someone may need to limit the amount of time they use technology e.g. I can suggest strategies to help with limiting this time.</p>	<p>Term 1.1 Health and Wellbeing I can describe ways that technology can affect health and well-being both positively (e.g., mindfulness apps) and negatively. I can describe some strategies, tips or advice to promote health and well-being with regards to technology. I can recognise the benefits and risks of accessing information about health and well-being online and how we should balance this with talking to trusted adults and professionals I can explain how and why some apps and games may request or take payment for additional content (e.g. in-app purchases, loot boxes) and explain the importance of seeking permission from a trusted adult before purchasing</p>	<p>Term 1.1 Health and Wellbeing I can describe common systems that regulate age related content (e.g. PEGI, BBFC, parental warnings) and describe their purpose I recognise and can discuss the pressures that technology can place on someone and how/when they could manage this. I can recognise features of persuasive design and how they are used to keep users engaged (current and future use) I can assess and action different strategies to limit the impact of technology on health (e.g. night-shift mode, regular breaks, correct posture, sleep, diet and</p>

PROCEDURE E-SAFETY (DIGITAL AND ONLINE)	Owner	E-Safety (Digital and Online) Leads
	ID (Version)	DU/5.1.1.3 (v3)
	Published	15 August 2024
	Valid Until	15- August 2025 (Annual)

<p>Term 1.2 Online Reputation I can recognise that information can stay online and could be copied I can describe what information I should not put online without asking a trusted adult first</p>	<p>Term 1.2 Online Reputation I can explain how information put online about someone can last for a long time I can describe how anyone's online information could be seen by others I know who to talk to if something has been put online without consent or if it is incorrect.</p>	<p>Term 1.2 Online Reputation I can explain how to search for information about others online • I can give example of what anyone may or may not be willing to share about themselves online. I can explain the need to be careful before sharing anything personal • I can explain who someone can ask if they are unsure about putting something online.</p>	<p>Term 1.2 Online Reputation I can describe how to find out information about others by searching online. • I can explain ways that some of the information about anyone online could have been created, copied or shared by others</p>	<p>Term 1.2 Online Reputation I can search for information about an individual online and summarise the information found. • I can describe ways that information about anyone online can be used by others to make judgements about an individual and why these may be incorrect.</p>	<p>Term 1.2 Online Reputation I can explain the ways in which anyone can develop a positive online reputation • I can explain strategies anyone can use to protect the 'digital personality' and online reputation, including degrees of anonymity.</p>
--	---	---	---	---	--

<p>Term 1.2 Copyright and Ownership I can explain why work I create using technology belongs to me I can say why it belongs to me (e.g. I designed it or I filmed it) I can save my work under a suitable title/name so that others know it belongs to me (e.g. filename, name on content) I understand that work made by others does not belong to me even if I save a copy.</p>	<p>Term 1.2 Copyright and Ownership I can recognise that content on the internet may belong to other people. I can describe why other people's work belongs to them.</p>	<p>Term 1.2 Copyright and Ownership I can explain why copying someone else's work from the internet without permission isn't fair and can explain what problems this might cause.</p>	<p>Term 1.2 Copyright and Ownership When searching on the internet for content to use, I can explain why I need to consider who owns it and whether I have the right to use it. • I can give some simple examples of content which I must not use without permission from the owner e.g., videos, music, images</p>	<p>Term 1.2 Copyright and Ownership I can assess and justify when it is acceptable to use the work of others. • I can give examples of content that is permitted to be reused and know how this content can be found online.</p>	<p>Term 1.2 Copyright and Ownership I can demonstrate the use of a search tool to find and access online content which can be reused by others. • I can demonstrate how to make references to and acknowledge sources I have used from the internet.</p>
<p>Term 2.1 Online Bullying I can describe how to behave online in ways that do not upset others and can give examples.</p>	<p>Term 2.1 Online Bullying I can explain what bullying is, how people may bully others and how bullying can make someone feel. I can explain why anyone who experiences bullying is not to blame. I can talk about how anyone experiences bullying can get help.</p>	<p>Term 2.1 Online Bullying I can describe appropriate ways to behave towards other people online and why this is important. • I can give examples of how bullying behaviour could appear online and how someone can get support.</p>	<p>Term 2.1 Online Bullying I can recognise when someone is upset, hurt or angry online. • I can describe ways people can be bullied through a range of media (e.g. image, video, text, chat) • I can explain why people need to think carefully about how content they post might affect others, their feelings and how it may affect how others feel about them (their reputation)</p>	<p>Term 2.1 Online Bullying I can recognise that online bullying can be different to bullying in the physical world and can describe some of those differences. • I can describe how what one person perceives as playful joking and teasing (including banter) might be experienced by others as bullying • I can explain how anyone can get help if they are being bullied online and identify when to tell a trusted adult. • I can identify a range of ways to report concerns and access support both in school and at home about online bullying. • I can explain how to block abusive users • I can describe the helpline services which can help people experiencing bullying, and how to access them (e.g. Childline or The Mix)</p>	<p>Term 2.1 Online Bullying I can describe how to capture bullying content as evidence (e.g., Screengrab, URL, profile) to share with others who can help me. • I can explain how someone would report online bullying in different contexts.</p>
<p>Term 2.1 Self Image I can recognise that there may be people online who could make someone feel, sad, embarrassed or upset. I can give examples of when and how to speak to an adult I can trust and how they can help</p>	<p>Term 2.1 Self Image I can explain how other people may look and act differently online and offline. I can give examples of issues that might make someone feel sad, worried, uncomfortable or frightened; I can give examples of how they might get help.</p>	<p>Term 2.1 Self Image I can explain what is meant by the term 'identity' • I can explain how people can represent themselves in different ways online. • I can explain ways in which someone might change their identity depending on what they are doing online (e.g., gaming; using an avatar; social media) and why</p>	<p>Term 2.1 Self Image I can explain how my online identity can be different to my offline identity. I can describe positive ways for someone to interact with others online and understand how this will positively impact on how others perceive them. • I can explain that others online can pretend to be someone else, including my friends, and can suggest reasons why they might do this.</p>	<p>Term 2.1 Self Image I can explain how identity online can be copied/ modified or altered. I can demonstrate how to make responsible choices about having an online identity, depending on context.</p>	<p>Term 2.1 Self Image I can identify and critically evaluate online content relating to gender, race, religion, disability, culture and other groups, and explain why it is important to challenge and reject inappropriate representations online. • I can explain the importance of asking until I get the help needed.</p>

PROCEDURE E-SAFETY (DIGITAL AND ONLINE)	Owner	E-Safety (Digital and Online) Leads
	ID (Version)	DU/5.1.1.3 (v3)
	Published	15 August 2024
	Valid Until	15- August 2025 (Annual)

<p>Term 3.1 Managing Online Information I can give simple examples of how to find information using digital technologies e.g. search engines, voice activated searching I know/understand that we can encounter a range of things online including things we like and don't like as well as things which are real or make believe/a joke I know how to get help from a trusted adult if we see content that makes us feel sad, uncomfortable, worried or frightened.</p>	<p>Term 3.1 Managing Online Information • I can use simple keywords in search engines • I can demonstrate how to navigate a simple webpage to get information I need (e.g. home, forward, back buttons; links, tabs and sections. • I can explain what voice activated searching is and how it might be used, and know it is not real person (e.g. Alexa, Google Now, Siri) • I can explain the difference between things that are imaginary, 'made up', or 'make believe' and things that are 'true' or 'real' • I can explain why come information I find online may not be real or true.</p>	<p>Term 3.1 Managing Online Information I can demonstrate how to use key phrases in search engines to gather accurate information online. • I can explain what autocomplete is and how to choose the best suggestion • I can explain how the internet can be used to buy and sell things • I can explain the difference between a belief, an opinion and a fact and give examples of how and where they might be shared online. E.g., in videos, memes, posts, news stories etc. • I can explain that not all opinions shared may be accepted as true or fair by others (E.g. monsters under the bed) • I can describe and demonstrate how we can get help from a trusted adult if we see content that makes us feel sad, uncomfortable, worried or frightened.</p>	<p>Term 3.1 Managing Online Information • I can analyse information to make a judgement about probable accuracy and I understand why it is important to make my own decisions regarding content and that my decisions are respected by others. • I can describe how to search for information within a wide group of technologies and make a judgement about the probable accuracy (e.g. social media, image sites, video sites) • I can describe some of the methods used to encourage people to buy things online (e.g. advertising offers; in app purchases; pop ups) and can recognise some of these when they appear online. • I can explain why lots of people sharing the same opinions or beliefs online do not make those beliefs or opinions true. • I can explain that technology can be designed to act like or impersonate living things (e.g. bots) and describe what the benefits and risks might be. • I can explain what is meant by fake news e.g. why some people will create stories or alter photographs and put them online</p>	<p>Term 3.1 Managing Online Information I can explain the benefits and limitations of using different types of search technologies e.g., voice activated search engine. I can explain how some technology can limit the information I am presented with e.g. voice-activated only giving one search result. • I can explain what is meant by 'being sceptical'; I can give examples of when and why it is important to be sceptical. • I can evaluate digital content and can explain how to make choices about what is trustworthy e.g. differentiating between adverts and search results. • I can explain key concepts including: information, reviews, fact, opinion, belief, validity, reliability and evidence. • I can identify ways the internet can draw us to information for different agendas, e.g. website notifications, pop-ups, targeted ads. • I can describe ways of identifying when online content has been commercially sponsored or boosted, (e.g. by commercial companies or by vloggers, content creators, influencers) • I can explain what is meant by the term 'stereotype', how 'stereotypes' are amplified and reinforced online, and why accepting 'stereotypes' may influence how people think about others. • I can describe how fake news may affect someone's emotions and behaviour and explain why this may be harmful.</p>	<p>Term 3.1 Managing Online Information I can explain what is meant by a 'hoax'. I can explain why someone would need to think carefully before they share. • I can explain how search engines work and how the results are selected and ranked. • I can explain how to use search technologies effectively. • I can describe how some online information can be opinions and can offer examples. • I can explain how and why some people may present opinions as facts; why the popularity of an opinion or the personalities of those promoting it does not necessarily make it true, fair or perhaps even legal. • I can define the terms 'influence', 'manipulation', and 'persuasion' and explain how someone might encounter these online (e.g. advertising and 'ad targeting' and targeting for fake news.) • I understand the concept of persuasive design and how it can be used to influence peoples' choices. • I can demonstrate how to analyse and evaluate the validity of facts and information and I can explain why using these strategies are important. • I can explain how companies and news providers target people with online news stories they are more likely to engage with and how to recognise this. • I can describe the difference between online misinformation and disinformation. • I can explain why information that is on a large number of sites may still be inaccurate or untrue. I can assess how this might happen (e.g., the sharing of misinformation or disinformation. • I can identify, flag and report inappropriate content.</p>
---	--	--	--	--	--

Year 7	Year 8	Year 9	Year 10
--------	--------	--------	---------

PROCEDURE E-SAFETY (DIGITAL AND ONLINE)	Owner	E-Safety (Digital and Online) Leads
	ID (Version)	DU/5.1.1.3 (v3)
	Published	15 August 2024
	Valid Until	15- August 2025 (Annual)

<p>Online Relationships</p> <p>I can explain the importance of having a choice and giving others a choice online.</p> <p>I can explain how and why people who communicate with others through online platforms may try to influence others negatively and I can offer examples. e.g. racist / homophobic comments, social influencers sharing weight loss products, grooming; radicalisation; coercion.</p> <p>I can explain strategies for assessing the degree of trust I place in people or organisations online.</p> <p>I can describe some signs of harmful online situations e.g. sexual harassment, grooming, cyberbullying.</p> <p>I can assess when I need to take action and explain what to do if I am concerned about my own or someone else's online relationship.</p>	<p>Online Relationships</p> <p>I can describe the benefits of communicating with a partner online.</p> <p>I can explain how relationships can safely begin (online dating), develop, be maintained, changed and end online.</p> <p>I can recognise harmful language of a discriminatory nature and harassment online and who can support people if this occurs (e.g. homophobia, name-calling, threatening to 'out' someone, threatening violence).</p> <p>I can describe different ways someone can give, gain or deny consent online and explain why context is important for assessing this.</p> <p>I can explain the differences between active, passive and assumed consent online.</p> <p>I can explain why we have a collective responsibility to gain consent before sharing or forwarding information online (e.g. personal details, images)</p> <p>I can give examples of how to make positive contributions to online debates and discussions.</p> <p>I can give examples where positive contributions have effected change in an online community.</p>	<p>Online Relationships</p> <p>I can give examples of how harmful online sexual behaviour can occur and can critically assess the potential harm.</p> <p>I can explain what is meant by making and sharing explicit images and videos (e.g. nudes and upskirting), I can identify different contexts in which this can happen (e.g. consensual, non-consensual), explain a range of possible impacts and identify strategies for seeking help.</p> <p>I can describe the laws that govern online behaviour and how they inform what is acceptable or legal (e.g. sexting and related terminology, trolling, harassment, stalking).</p>	<p>Online Relationships</p> <p>I can describe how online technology allows access to and communication with global communities.</p> <p>I can give examples of how anyone can adapt their behaviour to engage positively and sensitively with a diverse range of people, taking into account gender, cultural sensitivity, political and religious beliefs etc.</p> <p>I can explain how consent can be mistakenly assumed and demonstrate how to appropriately challenge this e.g. within established friendships, being generalised or having been previously given.</p> <p>I can recognise healthy and unhealthy behaviour in relationships and assess when the use of technology is becoming coercive and / or controlling (e.g. obsessive communication via online platform or text, using location apps to monitor and manipulate). I can explain when this is abusive, and strategies for getting help and support.</p>
<p>Privacy and Security</p> <p>I can explain why someone should use a strong and separate password for their email account, as the gateway to other online accounts.</p> <p>I can explain the terms 'connectivity' and the 'Internet of things'.</p> <p>I can recognise that devices can collect and share data about users with or without their knowledge or awareness, e.g. device usage including microphone, camera and geolocation.</p> <p>I understand the benefits of two factor authentication and use it where available.</p> <p>I can explain why backing up data is important and how this can be done.</p> <p>I can explain how and why it is important to always ensure someone makes safe and secure online payments.</p> <p>I can explain why online services have terms and conditions that govern their use and give examples that illustrate how they impact on a user e.g. age restrictions.</p> <p>I can explain what malware is and give some examples of how it operates and what the impact could be on a device or user (e.g. viruses, trojans, ransomware).</p> <p>I can explain what cookies are and can give examples of how my online browsing can be tracked and used by others (e.g. adware).</p> <p>I can explain that devices and the internet can be monitored in order to keep people safe.</p>	<p>Privacy and Security</p> <p>I can explain what cookies are and can give examples of how my online browsing can be tracked and used by others (e.g. adware).</p> <p>I know that accessing some websites or services may increase the risk of encountering viruses and other types of malware.</p> <p>I can demonstrate ways in which someone can change their browser settings to make their online browsing more secure (e.g. cookie permissions, do-not-track-me, password storage, incognito).</p> <p>I can explain app permissions and analyse them to make informed choices on which apps to use.</p> <p>I can explain how the security of devices connected to the internet may be compromised (e.g. webcams, monitors, phones or toys). I can demonstrate actions people can take to minimise such compromise (e.g., covering cameras on computers when not in use).</p>	<p>Privacy and Security</p> <p>I can identify choices and demonstrate strategies to control the personal data online services hold.</p> <p>I can explain why it's important to know how to recover a device or account if it gets compromised / hacked.</p> <p>I can explain that hacking can have legal consequences.</p> <p>I know who people can report to if they have experienced a cyber problem (e.g. identity theft, ransomware).</p>	<p>Privacy and Security</p> <p>I can contribute to an informed debate between national security and safeguarding as against personal privacy</p> <p>I can describe how data drawn from users of online services can be collected, used or sold to inform other services and organisations without the users' knowledge or consent. I can give examples of this.</p> <p>I can demonstrate additional ways to protect and manage data on my devices (e.g., find my phone; remote access; remote data deletion)</p>

PROCEDURE E-SAFETY (DIGITAL AND ONLINE)	Owner	E-Safety (Digital and Online) Leads
	ID (Version)	DU/5.1.1.3 (v3)
	Published	15 August 2024
	Valid Until	15- August 2025 (Annual)

<p>Health and Wellbeing I recognise and can discuss the pressures that technology can place on someone (e.g. immediate response on social media and messaging apps; always available; invasive; rapid engagement). I can explain the importance of self-regulating technology use; I can demonstrate strategies to do this (e.g. monitoring time spent online, avoiding accidents). I can explain how someone might recognise that they need support to manage their use of technology and who might provide that support. I can describe strategies to identify and assess when peers may need support and describe ways to assist peers who may be experiencing difficulties. I can identify commercial content (e.g. pop-ups, spam) and can discuss simple strategies to manage such content (e.g. pop-up blockers, junk folders, unsubscribing).</p>	<p>Health and Wellbeing I can assess the benefits of, and potential problems with, sites or apps that intend to promote positive well-being (e.g., wellness apps, fitness trackers, meditation/relaxation apps). I can demonstrate criteria for assessing and differentiating between health sites that offer unbiased, accurate and reliable health information from those promoting a product or agenda. I can describe the criteria to evaluate the benefits and risks associated with technology and apps available.</p>	<p>Health and Wellbeing I can identify online content and / or groups that promote unhealthy coping strategies (e.g. suicide, eating disorders, self-harm). I can identify and assess some of the potential risks of seeking help or harmful advice from these sites. I can identify who to talk to if I thought someone was at risk of being influenced by such sites. I know how to report content which is promoting unhealthy or harmful behaviour</p>	<p>Health and Wellbeing I can identify and assess features that might indicate that a site or social group could negatively impact on wellbeing I can offer strategies to identify and evaluate help from established respected sites or organisations that may be more helpful I can explain the benefits and risks of using online sources to self-diagnose and self-medicate and why someone should consult a medical professional if they are concerned about their health</p>
<p>Online Reputation I can describe and assess the benefits and the potential risks of sharing information online. I can explain how the information online services hold about someone forms part of their 'online identity' and how this differs from their digital personality. I can describe what is appropriate to say and do in different online settings / platforms (e.g., opinions, values, information, shares, 'likes', 'forwards').</p>	<p>Online Reputation I can explain and give examples of how what anyone writes online can also affect their school, family or social group, or future opportunities. I can describe ways that someone can manage what others can say and share about them and explain strategies to protect an individual's 'digital personality'.</p>	<p>Online Reputation I can monitor and manage my online reputation and I can describe clear steps to ensure that it promotes a positive image. I can identify some of the key laws governing online behaviour and reputation and the potential criminal implications of breaking them.</p>	<p>Online Reputation I can explain how aspects of someone's online identity can be linked together, and while something might be shared privately, it could have an impact later, personally and professionally I can explain the importance of someone's online reputation (especially to their future career) and can describe ways of managing this I can describe how to appropriately challenge content or behaviour that may have a negative impact on someone's online reputation</p>
<p>Copyright and Ownership I know that commercial online content can be viewed, accessed or downloaded illegally. I can give some examples of illegal access (e.g. illegal streaming, pirate sites, torrent sites, peer-to-peer sharing) and the associated risks. I can accurately define the concept of plagiarism. I can use this definition to evaluate online sources.</p>	<p>Copyright and Ownership I understand the concept of software and content licensing. I can understand and explain the principles of fair dealing and apply this to real case studies from my own research. I can identify the potential consequences of illegal access or downloading and how it may impact me and my immediate peers. I can explain why controlling copyright of my content may be limited when using social media, websites and apps.</p>	<p>Copyright and Ownership I understand Creative Commons Licensing protocols. I can demonstrate simple ways in which I can protect my own work from copyright theft. I can evaluate the possible impact of legal and illegal downloading on those people who create online content and the consequences for the wider community.</p>	<p>Copyright and Ownership I can apply Creative Commons Licensing to my own work</p>
<p>Online Bullying I can describe how bullying may change as we grow older and recognise when it is taking place online. I can describe a range of different bullying types and behaviours and assess when these are occurring (e.g. homophobia, racism, gender discrimination, sexism, ableism, exclusion of others from online forms of communication. setting up fake profiles of another person). I can explain why anyone experiencing online abuse is never to blame (e.g. victim blaming) and that to suggest they are is wrong. I can identify and demonstrate actions to support others who are experiencing difficulties online</p>	<p>Online Bullying I can explain my criteria for distinguishing between online bullying and teasing (banter) online. I can offer examples to differentiate between them. I can demonstrate how someone would intervene (and how they would assess if this should be directly or indirectly) to support others who are experiencing difficulties online. I can give examples of effective strategies which might help myself or others.</p>	<p>Online Bullying I can explain how cruelty and unpleasant comments can escalate quickly online. I can explain the concept of disinhibition online and can explain how this can be problematic. I can explain and assess a variety of routes to report bullying both in school and at home that include social reporting, peer support, anonymous reporting routes and helpline services. I can describe some of the laws that govern online behaviour and bullying and the potential implications of breaking them. I can explain what actions I can take if I believe these laws have been broken.</p>	<p>Online Bullying I can identify and assess behaviours that might be seen as bullying in different online contexts (e.g. close friendship groups vs public forums) and adjust my own behaviour accordingly</p>

PROCEDURE E-SAFETY (DIGITAL AND ONLINE)	Owner	E-Safety (Digital and Online) Leads
	ID (Version)	DU/5.1.1.3 (v3)
	Published	15 August 2024
	Valid Until	15- August 2025 (Annual)

<p>Self-Image I can give examples of how the internet and social media can be used for positive self-promotion. I can explain how anyone can curate and experiment with their identity online and why they might wish to do this. I am aware that a person's online activity, history or profile (their 'digital personality') will affect the type of information returned to them in a search or on a social media feed, and how this may</p>	<p>Self-Image I can assess the potential reputational benefits and risks in the way I represent myself online and explain strategies to manage this (e.g. anonymity, 'brand you'). I can explain what 'autonomy' means to me when it comes to the things I share and choose to engage with online. I can describe how messages online portraying 'identity ideals' can inhibit someone from being themselves online or sharing things openly. I can explain why it is important to balance 'keeping an open mind' with critically evaluating what ideas, opinions or beliefs I accept and reject and why I may need to re-evaluate if new evidence emerges. I can reflect on and assess the role that digital media plays in my life and give clear examples of where it benefits my lifestyle</p>	<p>Self-Image I can explain how online images can help to reinforce stereotypes. I can describe some of the pressures that people can feel when they are using social media (e.g. peer pressure, a desire for peer approval, comparing themselves or their lives to others, FOMO). I can explain how any images and videos can be digitally manipulated (e.g. using filters, cropping, deep fake technology).</p>	<p>Self-Image I can explain how online content can limit our autonomy by influencing peoples' thinking, feelings, beliefs, behaviours and responses; I can recognise and evaluate different factors and their impact. I can explain how online content can be shaped and targeted to influence body image, purchasing choices and behaviour (e.g. fashion, pornography, lifestyle sites and social media influencers). I can explain why some social media influencers promoting products and lifestyle can be virtual (computer generated personalities) and not real people. I can explain what is meant by artificial intelligence (AI) and how it can harvest my identity and shape my online experiences.</p>
<p>Managing Online Information I can explain why using various additional tools can refine my searches more effectively (e.g. search filters: size, type, usage rights etc.). I can explain how online content published by an individual can be interpreted differently by others. I can explain how 'liking', 'sharing' or 'forwarding' online content can change people's opinions of someone (e.g. contribute to or damage their online reputation). I can explain how 'online marketplaces' can enable small businesses or individuals to do business on a wider / global scale. I can assess the benefits and limitations of online commerce.</p>	<p>Managing Online Information I can navigate online content, websites or social media feeds using more sophisticated tools to get to the information I want (e.g. menus, sitemaps, breadcrumb-trails, site search functions). I can refine search phrases with additional functions (e.g. +, AND, *, NOT, * wildcard). I can explain how search engine rankings are returned and can explain how they can be influenced (e.g. commerce, sponsored results). I can use a range of features to query assure the content I access online (e.g. hits, likes, comments). I can analyse and evaluate the reliability and validity of online information based on content as well as appearance. I can explain why accurate information can be used in a false context to deliberately disinform. I can explain that whilst everyone is entitled to their opinion, not all opinions are equally credible or morally defensible (and some may be restricted from public expression: e.g. those that encourage racial or religious hatred).</p>	<p>Managing Online Information I can explain and recognise how social media can amplify, weaken or distort the apparent strength, validity, or popularity of sometimes extreme ideas, beliefs or opinions (e.g. an echo chamber). I can understand that individuals and organisations can be impersonated to deliberately mislead. I can explain how activity on social media may be contributed by social bots. I can explain deepfake technology and why this may be dangerous (e.g. for individuals and the democratic process). I can explain how accusations of fake news can be used to discredit the accurate reporting of real events.</p>	<p>Managing Online Information I can recognise when and analyse why online content has been designed to influence people's thoughts, beliefs or restrict their autonomy (e.g. fake/misleading reviews, fake news or propaganda). I can differentiate between genuine news sites and fake (or imitation) news sites with similar web addresses, and if uncertain, I can remain sceptical. I can explain why conspiracies based on disinformation may still attract people even without being grounded in real evidence. I can demonstrate the appropriate routes if I need to report illegal content e.g. social media reporting tools, government reporting sites (terror material)</p>

APPENDIX C: ARBOR SAFEGUARDING TEAM

Role	Person
Safeguarding Governor (DSG)	Kenneth Jones governors@thearborschool.ae
Arbor Principal	Gemma Thornley principal@thearborschool.ae
Designated Safeguarding Lead (DSL)	Frances Powell headofsecondary@thearborschool.ae
Deputy Designated Safeguarding Lead (DDSL)	Kathryn Keeshan headofprimary@thearborschool.ae
Designated Safeguarding Person (DSP)	PRIMARY: Richard Swingler rswingler@thearborschool.ae SECONDARY: Vanessa Mitchell vmitchell@thearborschool.ae NON-ACADEMIC: Ghadah AlSalous galsalous@thearborschool.ae
Deputy Designated Safeguarding Person (DDSP)	PRIMARY (EYFS): Chloe Morrith cmorrith@thearborschool.ae PRIMARY (KS1): Megan Gallacher mgallacher@thearborschool.ae PRIMARY (KS2): Evelyn Henderson ehenderson@thearborschool.ae SECONDARY (KS3): Nicholas Cooke ncooke@thearborschool.ae SECONDARY (KS4): Emily Kerr Laslett ekerrlaslett@thearborschool.ae SECONDARY (KS5): Chris Martin cmartin@thearborschool.ae LSAs: Janice Quinto jquinto@thearborschool.ae NON-ACADEMIC: Luda Zuhair lzuhair@thearborschool.ae
Thrive Representative	Sarah Vundum svundum@thearborschool.ae

PROCEDURE E-SAFETY (DIGITAL AND ONLINE)	Owner	E-Safety (Digital and Online) Leads
	ID (Version)	DU/5.1.1.3 (v3)
	Published	15 August 2024
	Valid Until	15- August 2025 (Annual)

Family Liaison	Ashleigh Wilson awilson@thearborschool.ae
Counsellors	Alexandra Jurgensen ajurgensen@thearborschool.ae Jacqueline Harrison jharrison@thearborschool.ae
Medical	Dr Quratulain Faisal qfaisal@thearborschool.ae
E-Safety (Digital and Online) Leads	PRIMARY: Sabrina Michael smichael@thearborschool.ae SECONDARY: David Smale dsmale@thearborschool.ae NON-ACADEMIC: Ali Hatamleh a.hatamleh@mgtt.com