



MAIDA VALE SCHOOL

Online Safety Policy

Date of issue:	September 2026
Renewal date:	September 2027
Individual Responsible:	Toby Fisher, Senior Deputy Head
Approved by:	Board of Directors

Contents

1. Introduction and Scope	3
2. Aims	3
3. Roles and Responsibilities	4
4. Understanding Online Risk: The Four Cs	6
5. Filtering and Monitoring	6
6. Artificial Intelligence	8
7. Cyber Security	9
8. Acceptable use of School Systems	10
9. Mobile Phones	12
10. Photography, Video and Imagery, including Nudes and Semi-Nudes	13
11. Online Bullying, Abuse and Exploitation	14
12. The Online Safety Act 2023: What Students and Parents can Expect from Platforms	15
13. Education and the Curriculum	16
14. Working with Parents and Carers	16
15. Recording, Reporting and Responding to Concerns	17
16. Review of this Policy	17
Appendix 1: Acceptable Use Agreement - Students	18
Appendix 2: Acceptable Use Agreement — Staff, Governors and Contractors	20
Appendix 3: Acceptable Use Agreement — Visitors and Volunteers	21
Appendix 4: Useful Links and Reporting Routes	22

This policy takes account of guidance from the DfE, ISI, ISBA, UKCIS, Ofcom and the NCSC. It is published on the school website; further copies are available to parents and students on request.

This policy should be read alongside:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Policy on Searching, Screening and Confiscation
- Data Protection Policy and Privacy Notices
- Staff Code of Conduct
- Acceptable Use Agreements (Appendices 1–3 of this policy)

Where this policy and the Safeguarding and Child Protection Policy appear to differ, the Safeguarding and Child Protection Policy takes precedence and the discrepancy must be reported to the DSL for correction.

1. Introduction and Scope

The internet and connected technology are an essential part of education and of everyday life for our students, in and out of school. The school has a duty to provide good quality, safely filtered access as part of students' learning, and a duty to educate students so that they understand the risks they encounter, can evaluate what they see, and can look after their own safety, security and wellbeing online.

Technology at Maida Vale School is used to enhance teaching and learning, to raise standards, to develop independent learning and intellectual curiosity, and to support the professional work of staff and the management of the school.

Scope. This policy applies to all students, staff, governors, volunteers, contractors and visitors who use the school's IT systems or who use any device — school-owned or personal — on school premises. It also applies to online conduct outside school where that conduct affects the wellbeing of a member of the school community or the reputation of the school. Online safety incidents that occur outside school and outside school hours will be dealt with under this policy and the Behaviour and Anti-Bullying Policies.

Online safety is a safeguarding matter, not solely a technical one. Where online activity raises a concern about the welfare of a child, staff must follow the Safeguarding and Child Protection Policy without delay.

2. Aims

- To enable students to take full advantage of the educational opportunities that technology provides.
- To develop in students the behaviours and critical thinking skills they need to stay safe and within the law online, in and beyond the classroom.
- To help students understand the range of risks in the digital world — including harmful content, contact from adults and peers who wish to harm them, harmful conduct by and towards others, and commercial and financial exploitation — and to take responsibility for their own online safety.
- To safeguard students from online bullying, abuse, exploitation and harm of any kind.

- To provide appropriate filtering and monitoring, to know how effective it is, and to be able to demonstrate that we have checked.
- To set clear expectations for the safe, responsible and lawful use of artificial intelligence by students and staff.
- To protect the school's data, systems and community from cyber attack.
- To ensure staff and students comply with copyright, data protection and other relevant law.
- To clarify roles and responsibilities, and to explain how the school responds to breaches.

3. Roles and Responsibilities

3.1 Safeguarding leadership

Online safety sits within the school's wider safeguarding arrangements and therefore within the responsibilities of those staff with designated safeguarding roles:

Name	Title	Email	Phone
Mr Magnus Bashaarat	Headmaster	hmpa@maidavaleschool.com	020 4511 6000
Mr Toby Fisher	Senior Deputy Head and Designated Safeguarding Lead (DSL)	toby.fisher@maidavaleschool.com	020 4511 6000
Ms Dena Deedat	Head of Sixth Form and Deputy Designated Safeguarding Lead (DDSL)	dena.deedat@maidavaleschool.com	020 4511 6000
Mr Matthew Greenfield	Head of Year 7 & 8 and Deputy Designated Safeguarding Lead (DDSL)	matthew.greenfield@maidavaleschool.com	020 4511 6000
Ms Millie Pocock	Head of Year 9 and Deputy Designated Safeguarding Lead (DDSL)	millie.pocock@maidavaleschool.com	020 4511 6000
Ms Kate Ware	Head of Year 10 & 11 and Deputy Designated Safeguarding Lead (DDSL)	kate.ware@maidavaleschool.com	020 4511 6000

The DSL has lead responsibility for online safety. In line with KCSIE, the DSL must understand the filtering and monitoring systems in place, the processes that sit around them, and the roles and responsibilities of staff in relation to them. This responsibility is reflected in the DSL's job description.

3.2 Filtering and monitoring: named responsibility

Role	Named post holder	Responsibility
------	-------------------	----------------

SLT member responsible for filtering and monitoring	Ms Dena Deedat	Strategic ownership; leads the annual effectiveness review; reports to the governing body/proprietor; ensures records are kept
Designated Safeguarding Lead	Mr Toby Fisher	Safeguarding oversight of blocklists and monitoring alerts; decides on safeguarding responses; supports the annual review
IT Lead	Mr Hitesh Bhojani	Day-to-day technical operation, configuration and testing of filtering and monitoring; maintains logs; supports the annual review
Managing Director	Mr Theo Brehony	Ensures appropriate systems are in place, that effectiveness is reviewed at least once every academic year, and that the review is recorded

These are named roles, not delegable in their entirety to an external supplier. The school remains accountable for the effectiveness of its systems.

3.3 Students

Filters, firewalls and adult vigilance all matter, but the most durable protection is a student's own judgement. Students are responsible for their conduct online just as they are in lessons and around the school. Use of technology must be safe, responsible, respectful and legal.

Sanctions. Any misuse of technology, inside or outside school, will be dealt with under the school's Behaviour Policy, which sets out the school's staged response and the sanctions available. This policy does not set out a separate tariff of sanctions. Sanctions may also be applied to any student responsible for material on their own or another person's site or account that would breach school rules in any other context. In the most serious cases the Headmaster may impose any sanction that is proportionate, including permanent exclusion.

Where conduct amounts to bullying, the Anti-Bullying Policy applies. Where it raises a safeguarding concern, the Safeguarding and Child Protection Policy applies.

3.4 Staff

All staff have a responsibility to model, promote and support safe online behaviour, to follow this policy and the Staff Code of Conduct, and to report concerns to the DSL immediately.

All staff receive online safety training at induction and at least annually thereafter, as part of safeguarding and child protection training. This training includes the expectations, roles and responsibilities that apply to filtering and monitoring, how to report a filtering or monitoring problem, and the risks associated with generative AI.

All staff must sign the Acceptable Use Agreement at Appendix 2 before being given access to school systems, and again whenever it is materially revised.

3.5 IT staff and providers

The IT lead and the school's IT service provider are responsible for the technical operation, security and resilience of school systems, for implementing and testing filtering and monitoring, for maintaining logs, for applying security patching and access controls, and for reporting technical concerns to the SLT member responsible for filtering and monitoring and, where safeguarding is engaged, to the DSL.

3.6 Parents and carers

Parents and carers are partners in online safety. Their responsibilities are set out at section 14.

4. Understanding Online Risk: The Four Cs

The school uses the framework set out in KCSIE to categorise online risk. Staff training, curriculum coverage, risk assessment and incident recording all use these four categories.

Content — being exposed to illegal, inappropriate or harmful material. Examples: pornography; fake news and disinformation; racist, misogynistic or extremist material; content promoting self-harm, suicide or eating disorders; content glorifying violence; AI-generated content that is false, harmful or misleading.

Contact — being subjected to harmful online interaction with other users. Examples: peer-to-peer pressure; adults posing as children or young adults with the intent to groom or exploit; commercial advertising and unwanted contact; contact through games, livestreams, group chats and direct messaging.

Conduct — personal online behaviour that increases the likelihood of, or causes, harm. Examples: sharing or generating nudes and semi-nudes (including AI-generated images); online bullying; sharing another person's personal information; producing or sharing harmful content; behaviour that would be a criminal offence offline.

Commerce — risks such as online gambling, inappropriate advertising, phishing, fraud, in-game purchasing and loot boxes, financially motivated sextortion, "money mule" recruitment, and scams targeting young people. Staff who become aware that a student may be at risk in this way must report it to the DSL, who will consider a referral to the Anti-Phishing Working Group, Action Fraud or the police as appropriate.

5. Filtering and Monitoring

5.1 The standards we work to

The school's arrangements are designed against:

- the **DfE filtering and monitoring standards** for schools and colleges (one of the six core digital and technology standards);
- the **DfE Digital and technology standards in schools and colleges**;
- the **Plan technology for your school** self-assessment service, which the school completes and uses to identify gaps and to plan improvement; and
- KCSIE, which requires appropriate filtering and monitoring to be in place, its effectiveness to be reviewed **at least once every academic year**, and the school to be able to **demonstrate that those reviews have taken place**.

The school records the outcome of its Plan technology for your school self-assessment, retains it, and reports material gaps to the governing body/proprietor with a costed plan and timescale.

5.2 What we filter and monitor

The school provides filtered internet access using Sophos web filtering. Sites visited and searches made are logged and can be attributed to a user account or, on the student wireless network, to the MAC address of the connecting device.

Filtering and monitoring apply to all users, all school-owned devices, and all devices connected to the school network, including personal devices. Filtering is designed to block illegal content (including that identified by the Internet Watch Foundation and the police-assessed list of unlawful terrorist content) and content that is harmful or inappropriate in an educational setting, while not being so restrictive that it prevents legitimate teaching and learning.

Filtering is not a guarantee. No system blocks everything, and the more determined the search, the more likely it is that something gets through. Anyone — student or member of staff — who encounters harmful, illegal or inappropriate content must report it to a member of staff or to the IT lead immediately. Reporting content is never treated as an admission of wrongdoing where it was encountered inadvertently.

5.3 Monitoring alerts: who reviews them, and how quickly

Alert Level	Examples	Who reviews	Response time
Level 1 – Critical	Indicators of imminent risk to life or serious harm: suicide or self-harm intent, sexual abuse, exploitation, extremism, weapons	DSL (or DDSL in the DSL's absence), notified immediately by the IT lead or provider	Reviewed immediately on receipt during the school day; out of hours, at the start of the next school day, with the DSL contactable via the school's out-of-hours safeguarding route
Level 2 – Safeguarding	Repeated searching on harmful topics; bullying indicators; contact risk; disordered eating; gambling	DSL or DDSL	Within one school day
Level 3 – Behaviour / acceptable use	Attempts to bypass filtering; inappropriate but non-safeguarding searching; misuse of accounts	SLT member responsible for filtering and monitoring, with the relevant Head of Year	Within two school days
Level 4 - Technical	Filtering failures, misclassification, over-blocking, device faults	IT lead / provider	Within five school days , or immediately where a filtering failure is exposing students to harmful content

Escalation

Any alert that a member of staff, the IT lead or the IT provider believes may indicate a risk to a child is escalated to the DSL immediately, regardless of the level it was initially assigned. IT staff and providers do not make safeguarding decisions; they pass concerns on to the DSL. Where the DSL judges a concern to meet the threshold, a referral is made to children's social care or the police in accordance with the Safeguarding and Child Protection Policy.

All alerts reviewed, the decision made and the action taken are recorded on MyConcern. Records of monitoring alerts and their handling form part of the evidence for the annual review at 5.4.

5.4 Annual review of effectiveness

At least once every academic year, and following any significant change to systems, provision or risk, the school reviews the effectiveness of its filtering and monitoring. The review is:

- led by the SLT member responsible for filtering and monitoring;
- supported by the DSL (safeguarding perspective) and the IT lead or provider (technical perspective);
- reported to the governing body/proprietor.

The review considers, as a minimum: the risk profile of the school and its students; the categories of content blocked and whether they remain appropriate; testing of the filtering across different devices, user groups and networks; the volume, type and handling of monitoring alerts; incidents that filtering or monitoring failed to prevent or detect; the effectiveness of over-block and under-block reporting routes; whether staff and students know how to report; the adequacy of training; and progress against the DfE standards and the Plan technology for your school self-assessment.

The review is recorded in writing using the template at Appendix 4. Records are retained and available for inspection.

5.5 Reporting a filtering or monitoring problem

Staff and students should report:

- content that should have been blocked but was not, and
- legitimate educational content that is blocked but should not be,

to the IT lead in the first instance, and to the DSL where the content is harmful. Reports of both kinds are logged and reviewed as part of the annual review. Over-blocking is treated as a genuine problem to be fixed, not an acceptable side effect.

6. Artificial Intelligence

Generative AI is now part of everyday life for students and staff. It offers real educational benefit and introduces real risk. This section sets out how AI is used and governed at Maida Vale School.

6.1 AI-specific risks

Deepfakes and AI-generated imagery. Creating, requesting, possessing or sharing manipulated or synthetic images or video of another person — student, staff member or anyone else — is a serious breach of discipline and may be a criminal offence. KCSIE now expressly includes AI-generated images and videos, including deepfakes, within the definition of child-on-child abuse, and the definition of a "nude or semi-nude" image includes images generated wholly or partly by AI. An AI-generated intimate image of a child is treated by this school exactly as a real one would be: it is reported to the DSL immediately and handled under section 10 of this policy and the Safeguarding and Child Protection Policy.

Nudification and undressing apps. Any use of an app or service that purports to remove clothing from an image of a real person is prohibited and will be treated as serious safeguarding and disciplinary matters, whoever the subject is.

Image harvesting. Students and parents should be aware that images shared publicly — including school photographs, sports pictures and social media posts — can be scraped and manipulated. Section 10 sets out the school's rules on photography and publication.

AI chatbots and companions. Chatbots can be persuasive, can produce false or harmful information with complete confidence, and can be designed to encourage prolonged engagement or emotional dependence. Students are taught that a chatbot is not a friend, not a counsellor and not a reliable source; that it may be designed to keep them talking; and that anything that worries them in a chatbot conversation should be reported to a member of staff. Staff must be alert to signs that a student is relying on an AI companion in place of human support, or is receiving harmful advice from one, and must report such concerns to the DSL.

Cognitive offloading. Habitual delegation of thinking to AI — for recall, reasoning, planning or writing — can weaken the very skills school exists to build. Teachers design tasks so that students do the cognitive work themselves where that work is the point of the task and are explicit with students about when AI use is and is not appropriate. Students are taught to use AI as a tool to check, extend or challenge their own thinking, not to replace it.

Bias, accuracy and disinformation. AI systems reproduce the biases of their training data and generate plausible falsehoods. Students are taught to verify AI output against reliable sources, and to recognise AI-generated text, images, audio and video.

See Group AI Policy for more details

7. Cyber Security

A cyber incident is a safeguarding risk as well as an operational one: compromised systems expose personal data about children.

The school works towards the DfE Cyber security standards for schools and colleges and the wider Digital and technology standards in schools and colleges. Cyber security is one of the six core standards that all schools are expected to meet by 2030. The six core standards are:

1. Broadband internet
2. Wireless networks
3. Network switching
4. Filtering and monitoring
5. Cyber security
6. Digital leadership and governance

The school's position against each is assessed using the Plan technology for your school service, recorded, and reported to the governing body/proprietor with a plan for any gaps.

7.1 Core controls

- Multi-factor authentication is in place wherever it is available, and in all cases on email, administrative accounts and remote access.
- Accounts and access are individual, are granted on a least-privilege basis, and are removed promptly when a person leaves or changes role. Administrative accounts are separate from everyday accounts.
- Patching and updates are applied promptly to all software, firmware and devices.
- Anti-malware and firewalls are deployed and kept current on school devices; personal devices connecting to the school network must have current anti-virus protection.
- Backups are taken regularly, held separately from the live environment, and tested by restoration.
- Training is provided at least annually to everyone with access to school systems, covering phishing and social engineering, password security, MFA, device security, removable media, and how to report a suspected incident or personal data breach.
- Incident response. The school has a cyber response plan forming part of its business continuity planning. Suspected incidents must be reported immediately to the IT lead and to [named senior leader]. Where personal data may have been compromised, the Data

Protection Policy applies and the ICO must be notified within 72 hours where the threshold is met. Cyber incidents are also reported to Action Fraud and, where relevant, the NCSC.

- Risk reporting. Cyber risks are reported to the governing body/proprietor as part of the school's risk management process.

7.2 Student Network Access and Authentication

Students access the school's wireless network using their individual school-issued username and password via the Sophos Captive Portal. Authentication is integrated with the school's identity management system, ensuring that network and internet access is attributable to a named user rather than a shared account.

This approach supports the school's safeguarding, filtering and monitoring responsibilities by providing individual accountability, enabling access to be controlled and revoked on a per-user basis, and allowing internet activity to be linked to authenticated users where required for safeguarding, security investigation, or incident response purposes.

The school does not use shared pupil credentials for internet access. Each user is responsible for maintaining the confidentiality of their account credentials and must not share them with others.

8. Acceptable use of School Systems

All users must sign the relevant Acceptable Use Agreement (Appendices 1–3) before being given access to school systems.

8.1 Passwords and account security

Staff have individual logins for the school network and iSAMS. All users must:

- use a strong, unique password, changed when prompted or when there is any reason to think it has been compromised;
- never write passwords down where they can be found, and never store them unencrypted;
- never share a password with anyone, including colleagues, family members or students;
- use multi-factor authentication where it is available;
- lock or log out of devices when leaving them unattended; and
- report any suspected compromise of an account immediately to the IT lead.

Using another person's account or password, or allowing another person to use yours, is a serious breach of this policy.

8.2 Prohibited use

No user of the school network or internet connection may:

- retrieve, create, send, copy, store or display offensive, obscene, discriminatory or otherwise inappropriate material;
- use obscene, racist, misogynistic or otherwise discriminatory language;
- harass, insult, threaten or attack others;
- damage, disrupt or attempt to gain unauthorised access to computers, systems or networks, or attempt to bypass filtering or monitoring (including by VPN, proxy, tethering to a personal hotspot, or use of an unapproved browser);

- violate copyright, or breach licensing terms;
- use another user's password or account, or access another user's folders, work or files;
- use the network for commercial or private business purposes;
- install software or hardware on a school device without authorisation;
- share or distribute executable files, copyrighted media, pornography, or material encouraging terrorism or radicalisation, whether by email, messaging, file sharing, AirDrop or by hosting files on a personal device;
- intentionally waste limited resources; or
- use school systems for private purposes without the express permission of the Headmaster or another senior member of staff.

All users must comply with the law on copyright, defamation, fraud, data protection, discrimination, obscenity and the Computer Misuse Act 1990.

8.3 Email

- Staff must use school email accounts to communicate with students. Communication must always be professional in tone, content and motivation, and must never take place through personal accounts or personal messaging apps.
- Students must tell a member of staff immediately if they receive offensive, threatening or upsetting email.
- Students must not disclose personal details about themselves or others by email, or arrange to meet anyone they have met online without the knowledge and permission of a parent.
- Email to external organisations should be written with the same care as a letter on school headed paper, and authorised where appropriate.
- Phishing is the most common route into school systems. Staff and students must not click links or open attachments in unexpected messages, and must report suspected phishing to the IT lead.

8.4 Social media and online publishing

Students and staff should understand how easy it is to publish personal information, and how difficult it is to remove it.

- Staff must be aware of the risks of social media and personal publishing, both professionally and personally, and must follow the Staff Code of Conduct. Staff must not run social media accounts or spaces for student use on a personal basis, and must not accept or initiate personal connections with current students.
- Students are advised not to give out information that identifies them or their location: real name, address, phone numbers, school, email and messaging handles, full names of family and friends, or specific clubs and routines.
- Students are advised to keep accounts private, to set strong passwords, to accept contact only from people they know in real life, and to know how to block and report.
- Students are advised not to publish private thoughts, and never to publish material that is threatening, hurtful or defamatory.
- Content that, in the reasonable opinion of the school, is offensive or defamatory to an individual or to the school is a serious breach of discipline and will be dealt with under the Behaviour Policy, regardless of where or on what device it was created.

8.5 Personal devices

Students may bring personal devices such as laptops and tablets onto school premises with permission. Such devices remain the responsibility of their owners at all times and must be kept with the student or in a locked locker, and secured with a password or passcode.

- The school is not responsible for theft, loss or damage to personal devices.
- No device may be used to bully, harass or intimidate.
- No device brought into school may contain pornography, extreme or violent material, or other material inappropriate in a school context.
- Personal devices must run current anti-virus software and must be kept updated.
- Students may connect to the school network only through the designated student wireless network, and may not use another student's device without that student's permission.
- AirDrop and equivalent short-range sharing (AirDrop, Quick Share, Nearby Share, Bluetooth transfer) must be set to receive from contacts only, or switched off, while on school premises. Sending unsolicited images or files to another person's device is a serious breach of discipline; sending indecent images in this way may be a criminal offence.
- Audio must be muted during the school day unless a teacher directs otherwise.
- Games must not be played in lessons, study periods, lunchtime sessions or after-school clubs unless a teacher has specified it as part of the work. Games must be age-appropriate; staff may require a student to remove a game that is not.
- The school may examine a personal device where there is reasonable suspicion that it is being used for an inappropriate or unlawful purpose, in accordance with the Policy on Searching, Screening and Confiscation and section 10.4 below.

8.6 School devices

School devices must be used for educational purposes and, where students are using them, under the supervision of a member of staff. Uploading inappropriate images, software or graphics is forbidden, including altering screensavers and backgrounds.

9. Mobile Phones

Maida Vale School is a phone-free school. This reflects both our own judgement and the DfE's expectation, given statutory force from 2026, that schools should be phone-free environments by default, with students prevented from accessing phones during lessons, breaks, lunchtimes and the time between classes.

We work with Yondr, which provides secure pouches used in over 3,000 schools across eighteen countries. Every student secures their phone in a labelled Yondr pouch on arrival at school. Students keep possession of their own phones throughout the day; the pouches are opened at the end of the school day. This applies to students in Years 7–11. Sixth Form students are not required to use Yondr pouches, but they must not use phones in front of younger students (including in lessons, corridors, or outdoor areas) and they may use phones in the Independent Learning Centre during break and lunch.

This arrangement for sixth form students is a justified exception with the rationale that the approach balances discipline with independence, helping older students develop responsible phone use in preparation for life beyond school, and any phone use is out of sight of the younger students. This exception was implemented in April 2026, when the new guidance was issued, but will be reviewed annually for its effectiveness.

We recommend that Year 7 students do not have a smartphone. Where a family judges a phone to be necessary, we recommend a device that makes and receives calls and texts only. Pouches are used for any phone, smart or not; a family whose child does not bring a phone does not need to buy a pouch.

Our aim is an environment in which students can concentrate on their work and on each other, and in which they can develop a healthier relationship with their devices. Learning and social behaviour improve markedly when students are fully engaged with their teachers and classmates.

The high value of phones, the cameras built into them, and the ease of using them discreetly all create risk; sections 8 and 10 of this policy apply to phones as to any other device.

10. Photography, Video and Imagery, including Nudes and Semi-Nudes

10.1 Taking and sharing images

- Photographs and video of any person on school premises must not be taken without that person's express permission. Even with permission, images must never be used to ridicule, harass, bully or abuse.
- Using images to harass, intimidate, ridicule or bully a student or member of staff is a serious breach of discipline.
- Uploading images to social media or video-sharing platforms which, in the reasonable opinion of the school, are offensive is a serious breach of discipline, whatever device was used and wherever it happened.
- Upskirting — taking an image beneath a person's clothing without their knowledge, for sexual gratification or to cause humiliation, distress or alarm — is a criminal offence under the Voyeurism (Offences) Act 2019.
- Editing, manipulating or using AI to alter an image of another person in a sexual, humiliating or degrading way is prohibited and may be a criminal offence (see section 6).

10.2 Nudes and semi-nudes shared by children — what staff must do

The making, possession or distribution of an indecent image of a child is a criminal offence under the Protection of Children Act 1978 and the Criminal Justice Act 1988, including where the image is of the child who made or shared it, and including images generated wholly or partly by AI.

The school follows the UKCIS/DfE guidance Sharing nudes and semi-nudes: advice for education settings working with children and young people, and the Safeguarding and Child Protection Policy.

If a member of staff is told about, or becomes aware of, an incident involving nudes or semi-nudes, they must:

1. Report it to the DSL immediately. The DSL, not the reporting member of staff, decides on the response.
2. Not view the imagery. Staff must not view, copy, print, share, store or save the imagery. If a member of staff has already viewed it inadvertently, they must record that fact and tell the DSL.
3. NOT DELETE THE IMAGERY, AND NOT ASK THE STUDENT TO DELETE IT. The imagery may be evidence. Deleting it, or instructing a child to delete it, may destroy evidence and may obstruct a criminal or safeguarding investigation.
4. Not ask the student to describe what the imagery contains. The DSL will manage any conversation.

5. Confiscate and secure the device where appropriate, placing it in flight mode or turning it off, in accordance with the Policy on Searching, Screening and Confiscation. The device is not to be searched further.
6. Explain to the student that the concern must be passed on, and reassure them that they will be supported. Staff must not promise confidentiality.
7. Record the report in the school's safeguarding records.

The DSL will hold an immediate review, speak to those involved as appropriate, make a decision on whether to refer to children's social care and/or the police, and record the rationale for that decision. Not every incident requires a referral, but the decision is the DSL's to make and must be recorded.

Note for staff: an earlier version of this policy instructed students to delete images if asked to do so by staff. That instruction has been removed because it conflicted with the UKCIS/DfE guidance and with the school's Safeguarding and Child Protection Policy. Where this policy and the Safeguarding and Child Protection Policy differ, the Safeguarding and Child Protection Policy applies.

10.3 Support for students

A student who has shared an image, has been pressured into sharing one, or has had an image shared or generated without their consent, will be supported and not treated as a wrongdoer for having been victimised. Students and parents can request removal of imagery through the Report Remove service operated by Childline and the Internet Watch Foundation. The DSL will support any such request.

10.4 Searching devices

Where the school has reasonable grounds to believe that a device contains material that breaches school rules or may constitute evidence of a criminal offence, the Policy on Searching, Screening and Confiscation applies. The school may pass a device to the police for examination. Students must allow staff reasonable access to material stored on a device where a search is properly authorised under that policy. Staff must not delete material found on a device, or instruct a student to delete it, where it may be evidence.

11. Online Bullying, Abuse and Exploitation

11.1 Online bullying

Students must not use their own or the school's devices to bully anyone, inside or outside school. Bullying incidents involving technology are dealt with under the Anti-Bullying and Behaviour Policies. A student who believes they or someone else is being bullied should tell a member of staff as soon as possible.

Online bullying is different from other bullying: it can follow a child home, it can be anonymous, it can reach a large audience instantly, and the material can be difficult to remove. A child being bullied through phones, games or the internet can feel very isolated, particularly if the adults around them do not understand how it works.

Online bullying commonly occurs through:

- group chats on messaging platforms, including exclusion from them and the sharing of screenshots taken out of context;
- gaming platforms, including in-game chat, voice channels and harassment during play;
- community platforms such as Discord, including private servers set up to target an individual;
- livestreaming, including streaming someone without their consent, coordinated abuse in live chat, and pressure to perform on camera;

- social media, including anonymous accounts, "hate pages", and coordinated pile-ons;
- AirDrop and short-range sharing, used to send unwanted images to nearby devices;
- AI-manipulated images and audio used to humiliate.

Online bullying will not be tolerated, whether it originates inside or outside school. Activity conducted outside school premises and hours that in our opinion constitutes online bullying is covered by this policy. The school will take reasonable steps to identify those responsible, which may include examining system logs, identifying and interviewing witnesses, and contacting the service provider and the police.

Responses, applied through the Behaviour and Anti-Bullying Policies, may include informing parents, withdrawal of privileges, requiring removal of material, and, in the most serious cases, permanent exclusion. Where a criminal offence may have been committed, the police will be contacted.

11.2 Financially motivated sextortion

Financially motivated sextortion — where a criminal, often part of an organised group operating from overseas, tricks or coerces a young person into sending an intimate image and then threatens to share it unless money is paid — is a fast-growing threat and disproportionately targets teenage boys. Offenders typically make contact through social media or gaming platforms, move quickly to private messaging, may use a fake or stolen profile, and escalate to threats within hours.

Students are taught that:

- it is not their fault, and they are not in trouble;
- they should not pay — paying does not stop the threats;
- they should stop communicating, take screenshots of the account and messages, block the account and report it to the platform; and
- they should tell a trusted adult immediately — a parent, a member of staff, or the DSL.

Staff who become aware of a sextortion concern must report it to the DSL immediately and must follow the steps at 10.2. The DSL will consider a report to the police and to the NCA's CEOP Safety Centre, and will support the student, who is a victim of crime.

11.3 Grooming, exploitation and radicalisation

If there is any suggestion that a student is at risk of abuse, exploitation or radicalisation arising from online activity, the matter is dealt with under the Safeguarding and Child Protection Policy and, where relevant, the school's Prevent duty arrangements. Any student worried about something they have seen or experienced online must report it to a member of staff as soon as possible.

12. The Online Safety Act 2023: What Students and Parents can Expect from Platforms

The Online Safety Act 2023 places legal duties on search services and on services that allow users to post content or interact with each other. Ofcom is the regulator and has powers to fine companies up to £18 million or 10% of global revenue.

Since the Protection of Children Codes of Practice came into force in July 2025, services likely to be accessed by children have been required to:

- carry out a children's risk assessment and keep it under review;
- prevent children from encountering the most harmful content — pornography, and content promoting suicide, self-harm or eating disorders;

- protect children from other harmful content, including bullying, abusive and hateful material, violent content and dangerous challenges;
- use highly effective age assurance where the service hosts or disseminates content harmful to children, rather than relying on a self-declared date of birth;
- configure recommender systems so that harmful content is filtered out of children's feeds where the service is medium or high risk;
- provide easy-to-use reporting and complaints routes, and act on reports; and
- publish clear terms of service and enforce them.

What this means in practice. Platforms are increasingly asking users to verify their age, and pornography sites in the UK are now expected to run effective age checks. Enforcement is active and ongoing, and Ofcom has reported that implementation remains uneven. The Act does not make the internet safe; it raises the floor. Parents should continue to use device- and account-level parental controls, and students should continue to report anything that troubles them.

Reporting. Students and parents should use the platform's own reporting tools in the first instance. Complaints about a platform's failure to comply with its duties can be raised with Ofcom. Illegal images of children can be reported to the Internet Watch Foundation; online sexual abuse or grooming can be reported to CEOP.

The legislative and regulatory position continues to develop. The school will keep this section under review at each annual policy review.

13. Education and the Curriculum

Online safety is taught through PSHE and the RSHE curriculum, through the computing and wider curriculum, through assemblies and tutor time, and through the pastoral system. Coverage is planned against the four Cs (section 4) and is age-appropriate and progressive across year groups.

Curriculum content includes: evaluating online information and recognising disinformation; understanding how algorithms and recommender systems shape what students see; privacy, data and digital footprint; healthy relationships online, consent and the law on image sharing; recognising grooming, exploitation and sextortion; online bullying and being an active bystander; gambling, in-game spending and financial scams; the impact of screen use on sleep, attention and wellbeing; and the safe, critical and honest use of generative AI.

Students are taught how to report — to the school, to platforms, and to external agencies — and are told repeatedly that they will not be in trouble for reporting something that has happened to them.

14. Working with Parents and Carers

KCSIE expects schools to reinforce online safety messages with parents. The school will:

- publish this policy and the student Acceptable Use Agreement on the school website, and provide copies on request;
- tell parents what students are being asked to do online, including the sites and platforms they will be asked to use, the AI tools approved for use, and the devices and accounts required;
- tell parents who students will be interacting with online in the course of school work, and the arrangements in place to keep those interactions safe;
- explain the school's filtering and monitoring arrangements, in outline, and what they do and do not cover — including that filtering does not extend to students' own devices on their own mobile data or at home;

- offer at least one parent information session each year on online safety, covering current risks and practical steps (device settings, parental controls, family agreements, conversations about AI, gaming and sextortion);
- communicate promptly with parents where an emerging risk affects the school community; and
- signpost parents to Internet Matters, the NSPCC, Childnet and the UK Safer Internet Centre (Appendix 5).

We ask parents and carers to:

- read and discuss the student Acceptable Use Agreement with their child, and sign it;
- support the phone-free school arrangements;
- take an active interest in what their child does online, including the games, platforms and chats they use, and who they talk to;
- use age ratings, parental controls and account settings, and keep devices out of bedrooms overnight where possible;
- talk to their child about sextortion, AI-generated images and pressure to share images, before something happens rather than after; and
- contact the DSL or their child's tutor promptly about any online concern, including concerns about incidents that happen entirely outside school.

15. Recording, Reporting and Responding to Concerns

- All online safety concerns, complaints and incidents are recorded on MyConcern. Reports of bullying are recorded under both the recipient's and the initiator's records.
- Concerns are categorised using the four Cs (section 4), which allows the school to identify patterns and target its education and filtering accordingly.
- Safeguarding concerns are reported to the DSL immediately and handled under the Safeguarding and Child Protection Policy.
- Behaviour breaches are dealt with under the Behaviour Policy; bullying under the Anti-Bullying Policy.
- Misuse may lead to confiscation of equipment in accordance with the Conducting a Search Policy and the Behaviour Policy.
- Allegations against staff arising from online conduct are handled under Part Four of KCSIE and the school's low-level concerns and allegations procedures.
- The DSL reports on online safety incidents, trends and actions to the SLT each term, and to the governing body/proprietor annually alongside the filtering and monitoring review.

16. Review of this Policy

This policy is reviewed annually by the Senior Deputy Head/ DSL, the SLT member responsible for filtering and monitoring, and the IT lead, and is approved by the Board of Directors. It will also be reviewed following any significant incident, any material change in technology or provision, or any change in statutory guidance.

The annual review of this policy is separate from, but informed by, the annual review of filtering and monitoring effectiveness required by KCSIE (section 5.4).

Next review due: September 2027

Appendix 1: Acceptable Use Agreement - Students

To be signed by every student and countersigned by a parent or carer on entry to the school and at the start of each academic year.

Name of student: **Form:**

I understand that the school provides me with technology and internet access to help me learn, and that the school monitors and filters what happens on its network and on its devices.

I agree that I will:

1. Use school technology for schoolwork, and only in the way my teachers have told me to.
2. Keep my password private, use a strong password, and never use anyone else's account.
3. Treat everyone with respect online, in exactly the way I am expected to in person.
4. Tell a member of staff straight away if I see anything online that upsets, worries or frightens me — at school or at home. I understand I will not be in trouble for reporting something.
5. Tell a member of staff straight away if I think someone is being bullied, pressured or harmed online.
6. Ask permission before taking a photograph or video of anyone, and never share an image of someone in a way that could embarrass, upset or humiliate them.
7. Keep my phone in my Yondr pouch during the school day.
8. Set AirDrop and similar sharing to "contacts only" or off while I am at school.
9. Use only the AI tools the school has approved, be honest about when I have used AI, and do my own thinking in my own work.
10. Respect other people's work and copyright, and not copy or share things I do not have permission to use.
11. Report anything that looks like a scam, a phishing message, or a request for money or images.

I agree that I will not:

12. Try to get round the school's filtering or monitoring, including by using a VPN, proxy or personal hotspot.
13. Look for, share, or store material that is violent, pornographic, hateful, extremist or otherwise inappropriate.
14. Bully, threaten, harass or exclude anyone online, or join in when someone else does.
15. Create, ask for, keep or share nude or semi-nude images of anyone, including myself, and including images made or altered using AI.
16. Use an app or website to alter an image of a real person to make it sexual, humiliating or degrading.
17. Give out personal information about myself or anyone else, or arrange to meet someone I only know online.

18. Damage school equipment, install software without permission, or access other people's files or accounts.

19. Use school systems to make money or run a business.

I understand that if I break this agreement, the school will deal with it under the Behaviour Policy, that my parents will normally be told, and that in serious cases the police may be involved.

Student signature: **Date:**

Parent/carers signature: **Date:**

Appendix 2: Acceptable Use Agreement — Staff, Governors and Contractors

To be signed on appointment, and whenever this agreement is materially revised.

Name: **Role:**

I have read the school's Online Safety Policy, Safeguarding and Child Protection Policy, Staff Code of Conduct and Data Protection Policy.

I agree that I will:

1. Use school systems and data lawfully, professionally and only for school purposes, except where personal use has been expressly permitted.
2. Use individual credentials, a strong unique password and multi-factor authentication where available; never share credentials; lock devices when unattended.
3. Communicate with students only through official school channels, never through personal accounts, personal phone numbers or personal messaging apps, and always in a professional tone.
4. Not accept or initiate personal social media connections with current students, and manage my own privacy settings so that my personal accounts are not accessible to students.
5. Report all safeguarding concerns to the DSL immediately, and follow the DSL's direction.
6. Follow the school's procedure on nudes and semi-nudes: report to the DSL; not view, copy, print, share, store or save the imagery; **not delete it and not ask a student to delete it**; secure the device without searching it further.
7. Store and transmit personal data only on approved systems, and never on unapproved cloud services, personal devices or unencrypted removable media.
8. Use only school-approved AI tools for school purposes, enter no personal data into any AI tool without an approved lawful basis, and take full professional responsibility for any AI-assisted output.
9. Model safe, respectful and critical use of technology to students.
10. Report suspected phishing, malware, lost or stolen devices, or any suspected data breach to the IT lead and DPO immediately.
11. Report filtering failures and over-blocking to the IT lead, and safeguarding-relevant content to the DSL.
12. Complete online safety, filtering and monitoring, data protection and cyber security training as required.
13. Respect copyright and licensing in all material I use or share.

I understand that:

- the school monitors and logs use of its systems and devices, and that I have no expectation of privacy in relation to school systems;
- breaches of this agreement may be dealt with under the school's disciplinary procedures and, where relevant, referred to the police, the ICO or the Teaching Regulation Agency.

Signature: **Date:**

Appendix 3: Acceptable Use Agreement — Visitors and Volunteers

To be provided and signed at reception before guest network access or device use on site.

Name:

Organisation:

Date of visit:

Host:

While on Maida Vale School premises I agree that I will:

1. Use the guest network only for lawful, appropriate purposes, and understand that my use is filtered and logged.
2. Not photograph, film or record any student or member of staff without the prior permission of my host, and not publish or share any such image.
3. Keep my mobile phone out of sight and unused in areas where students are present, except where my host has agreed it is necessary for my work.
4. Not attempt to access the school's internal network, systems or data.
5. Not connect storage devices to school equipment.
6. Report to my host or to reception anything I see online or in person that causes me concern about a child's welfare.
7. Not communicate with students online, or exchange contact details with a student.
8. Understand that the school's Safeguarding and Child Protection Policy applies to me, and that concerns about my conduct will be reported to the DSL.

Signature: **Date:**

Appendix 4: Useful Links and Reporting Routes

Statutory and departmental guidance

- Keeping children safe in education (KCSIE) — <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>
- Sharing nudes and semi-nudes: advice for education settings (UKCIS) — <https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people>
- Meeting digital and technology standards in schools and colleges — <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges>
- Filtering and monitoring standards — <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges>
- Cyber security standard — <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-core-standard>
- Plan technology for your school — <https://www.gov.uk/guidance/plan-technology-for-your-school>
- Generative AI: product safety expectations (updated January 2026) — <https://www.gov.uk/government/publications/generative-ai-product-safety-standards>
- Generative artificial intelligence (AI) in education — <https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education>
- Searching, screening and confiscation — <https://www.gov.uk/government/publications/searching-screening-and-confiscation>
- Teaching online safety in schools — <https://www.gov.uk/government/publications/teaching-online-safety-in-schools>

Reporting

- CEOP Safety Centre (online sexual abuse, grooming, sextortion) — <https://www.ceop.police.uk/safety-centre/>
- Internet Watch Foundation (illegal images of children) — <https://report.iwf.org.uk/>
- Report Remove (Childline/IWF — removal of a child's own images) — <https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/remove-nude-image-shared-online/>
- Report Harmful Content — <https://reportharmfulcontent.com/>
- Ofcom (online safety complaints) — <https://www.ofcom.org.uk/online-safety/>
- Action Fraud — <https://www.actionfraud.police.uk/>
- Childline — 0800 1111 — <https://www.childline.org.uk/>
- NSPCC Helpline — 0808 800 5000

Advice and education

- Childnet — <https://www.childnet.com/>

- Childnet online bullying resources (replaces the former digizen.org site, which is no longer available) — <https://www.childnet.com/help-and-advice/cyberbullying/>
- UK Safer Internet Centre — <https://saferinternet.org.uk/>
- Internet Matters (for parents) — <https://www.internetmatters.org/>
- Thinkuknow (NCA-CEOP education) — <https://www.thinkuknow.co.uk/>
- NSPCC online safety — <https://www.nspcc.org.uk/keeping-children-safe/online-safety/>
- National Cyber Security Centre — <https://www.ncsc.gov.uk/section/education-skills/schools>