



**EVERYTHING
EDUCATION**

ONLINE SAFETY POLICY

2026-2027

OWNERSHIP:	Everything Education School
AUTHORISED BY:	M Hussain (Headteacher)
EFFECTIVE FROM:	1/9/2026
REVIEW:	1/9/2027

Everything Education School

1234-1238 Coventry Road, Yardley, Birmingham B25 8BZ

CONTENTS

1.0 Purpose and Scope
2.0 Legal and Guidance Framework
3.0 Roles and Responsibilities
4.0 Online Safety Risks
5.0 Education and Curriculum
6.0 Filtering and Monitoring
7.0 School Devices, Networks and Accounts
8.0 Personal Devices and Mobile Phones
9.0 Social Media, Messaging and Online Communication
10.0 Generative Artificial Intelligence (AI)
11.0 Online Bullying, Sexual Harassment and Harmful Content
12.0 Safeguarding Concerns and Incident Response
13.0 Staff Use of Technology and Professional Conduct
14.0 Remote and Online Learning
15.0 SEND, EAL and Vulnerable Pupils
16.0 Data Protection, Privacy and Cyber Security
17.0 Parents, Carers and Partnership Working
18.0 Training, Monitoring and Review
Related Policies
Appendix 1 - Online Safety Incident Response Checklist
Appendix 2 - Filtering and Monitoring Review Checklist

1.0 PURPOSE AND SCOPE

Everything Education School is committed to providing a safe, respectful and educationally purposeful digital environment. Online safety is an integral part of safeguarding and applies whenever pupils or staff use technology in connection with the school, including school-managed devices, the school network, online platforms, remote learning and off-site use of school-managed technology.

The school recognises that technology provides significant opportunities for learning, communication, independence and preparation for adulthood, while also creating risks. Our approach is to protect pupils from harm, teach them to use technology safely and responsibly, and respond promptly to concerns without unnecessarily restricting legitimate teaching and learning.

This policy applies to pupils, staff, proprietors, volunteers, contractors and visitors where they use school systems or technology, or where online conduct has a safeguarding, welfare, behavioural or professional impact on the school community.

2.0 LEGAL AND GUIDANCE FRAMEWORK

This policy has regard to current legislation and statutory/national guidance, including:

- Keeping Children Safe in Education 2026 (KCSIE), in force from 1 September 2026;
- Education (Independent School Standards) Regulations 2014;
- Children Act 1989 and Children Act 2004;
- Equality Act 2010;
- UK GDPR and Data Protection Act 2018, as amended by relevant data legislation;
- Prevent duty guidance;
- DfE Filtering and Monitoring: Core Standard, updated 16 September 2026;
- DfE Meeting digital and technology standards in schools and colleges;
- DfE Data protection in schools guidance; and
- relevant legislation relating to communications, harmful content, harassment, sexual offences and misuse of computer systems.

Online safety should be read as part of the school safeguarding system and not as a separate technical issue. Where an online incident raises a safeguarding concern, the Safeguarding and Child Protection Policy takes precedence and the DSL will lead the safeguarding response.

3.0 ROLES AND RESPONSIBILITIES

3.1 PROPRIETOR

- has overall strategic responsibility for ensuring appropriate online safeguarding arrangements are in place;
- ensures appropriate filtering and monitoring systems are provided and their effectiveness is reviewed at least once every academic year;
- receives assurance that identified actions are addressed and that staff understand escalation routes; and
- ensures resources, training and technical support are proportionate to the school's pupil profile and use of technology.

3.2 HEADTEACHER

- implements this policy and ensures online safety is embedded across safeguarding, curriculum and staff practice;
- ensures roles for filtering, monitoring and incident response are clear;
- ensures staff receive appropriate information and training; and
- works with the DSL and IT support to review risks, incidents and controls.

3.3 DESIGNATED SAFEGUARDING LEAD (DSL)

- takes lead responsibility for safeguarding and child protection concerns arising from online activity;
- understands the filtering and monitoring arrangements and how concerns are escalated;
- reviews safeguarding alerts or reports as appropriate and ensures action is recorded; and
- supports staff, pupils and families where online harm is identified.

3.4 IT SUPPORT / TECHNICAL PROVIDER

- maintains agreed technical controls, user access and security arrangements;
- supports filtering and monitoring configuration and review;
- reports significant technical or safeguarding concerns promptly to the appropriate school lead; and
- does not make safeguarding decisions independently of the DSL or senior leadership.

3.5 ALL STAFF

- maintain appropriate supervision when pupils use technology;
- follow acceptable-use, safeguarding, data-protection and staff-conduct requirements;
- report online safety concerns to the DSL without delay;
- never investigate a safeguarding concern beyond what is necessary to establish immediate facts and safety; and
- model safe, lawful and professional digital behaviour.

4.0 ONLINE SAFETY RISKS

The school considers online safety through the commonly recognised areas of content, contact, conduct and commerce. Risks may include exposure to illegal or harmful material; misinformation or disinformation; pornography; self-harm or suicide content; extremist material; online bullying; grooming; exploitation; coercion; sexual harassment; sharing of nude or semi-nude images; scams; fraud; gambling; privacy breaches; impersonation; unsafe contact with strangers; harmful challenges; and inappropriate use of artificial intelligence.

Risk is considered in the context of each pupil. Age, developmental level, SEND, communication needs, EAL, emotional wellbeing, previous experiences, exploitation risks and the pupil's ability to recognise or report harm may all affect vulnerability.

5.0 EDUCATION AND CURRICULUM

Online safety education will be age-appropriate, developmentally appropriate and responsive to the needs of the school cohort. It will be reinforced through computing, PSHE/RSHE, safeguarding education, tutor/form time and relevant curriculum opportunities.

- privacy, passwords and personal information;
- healthy and respectful online relationships;
- consent, boundaries and image sharing;
- online bullying and reporting routes;
- recognising manipulation, grooming, exploitation and scams;
- critical evaluation of online information, misinformation and AI-generated content;
- copyright, plagiarism and responsible use of digital content;
- digital footprint, reputation and employability; and
- where and how to seek help.

6.0 FILTERING AND MONITORING

Everything Education School will maintain filtering and monitoring arrangements appropriate to its safeguarding duties, pupil risk profile and use of technology. Filtering is a preventative control intended to restrict access to illegal, inappropriate and potentially harmful content. Monitoring is a reactive safeguard used to identify concerning activity and support timely action.

- Filtering and monitoring responsibilities will be clearly assigned.
- Provision will be reviewed at least once every academic year and following significant change or a serious incident.
- The review will consider pupil age, SEND, EAL, risk profile, devices, locations, remote use, generative AI, safeguarding intelligence and teaching requirements.
- Filtering will apply to school-managed devices and school internet access, including guest access, as appropriate to the technical environment.
- Filtering will block illegal and harmful content without unreasonably restricting legitimate teaching and learning.
- Staff will supervise pupils using devices and will not rely solely on technical systems.
- High-risk alerts or concerns will be escalated promptly to the DSL or senior leader.
- Monitoring reports and incidents will be reviewed and actions/outcomes recorded.
- Any temporary filtering exception required for legitimate operational reasons must be authorised and documented by the appropriate senior leader.

No filtering or monitoring system can remove all risk. The school therefore combines technical controls with staff supervision, education, clear expectations and safeguarding response procedures.

7.0 SCHOOL DEVICES, NETWORKS AND ACCOUNTS

- Users must use school systems only for authorised educational or professional purposes.
- Passwords must be kept secure and must not be shared.
- Pupils must not attempt to bypass filtering, monitoring, security settings or access controls.
- Software, browser extensions or applications must not be installed without authorisation.
- School-managed devices must be configured and maintained with appropriate security controls.

- Lost, stolen or compromised devices/accounts must be reported immediately.
- Access rights will be proportionate to role and removed or changed when no longer required.

8.0 PERSONAL DEVICES AND MOBILE PHONES

Personal-device use by pupils is governed by the school's behaviour and mobile-phone arrangements. Where personal devices are permitted for a specific educational or welfare reason, this must be authorised and appropriately supervised. Personal devices must not be used to photograph, record or share information about pupils or staff without lawful authority and appropriate permission.

Staff must use school-approved systems for school business wherever required and must not use personal accounts or informal messaging channels to create inappropriate or unrecorded communication with pupils.

9.0 SOCIAL MEDIA, MESSAGING AND ONLINE COMMUNICATION

- Staff must maintain professional boundaries online and must not accept or initiate personal social-media relationships with pupils.
- School communications with pupils and families should use approved channels.
- Pupils will be taught that online abuse, threats, harassment, discriminatory language and non-consensual sharing are unacceptable.
- Concerns involving social media or messaging will be considered under safeguarding, behaviour, anti-bullying and staff-conduct procedures as appropriate.
- The school will preserve relevant evidence where safe and lawful to do so, while avoiding unnecessary viewing, copying or circulation of harmful material.

10.0 GENERATIVE ARTIFICIAL INTELLIGENCE (AI)

Generative AI may support teaching, learning and administration when used safely, lawfully and transparently. The school will assess safeguarding, data-protection, accuracy, bias, age-appropriateness and security risks before adopting AI products or requiring pupil use.

- Personal, confidential or special-category data must not be entered into unapproved AI tools.
- Pupils must not use AI to create harmful, sexual, abusive, discriminatory, deceptive or impersonating content.
- AI-generated outputs must be checked for accuracy and suitability and should not be treated as automatically reliable.
- Staff will make clear when and how AI may be used in assessed work and will address plagiarism or misrepresentation through school procedures.
- Filtering and monitoring reviews will consider dynamic and AI-generated content and any technical limitations of existing controls.

11.0 ONLINE BULLYING, SEXUAL HARASSMENT AND HARMFUL CONTENT

Online bullying and harmful sexual behaviour are treated seriously whether they occur on or off school premises where they affect a pupil's safety, welfare or education. The school will respond in a child-centred and proportionate way, taking account of the needs of all children involved.

Where concerns involve nude or semi-nude images, sexual harassment, exploitation or other potentially criminal conduct, staff must refer immediately to the DSL and follow safeguarding procedures. Staff must not routinely view, download, print, forward or store sexual imagery of children.

12.0 SAFEGUARDING CONCERNS AND INCIDENT RESPONSE

- Protect immediate safety and provide reassurance to the pupil.
- Report the concern to the DSL/DDSL without delay.
- Record factual information using the school safeguarding system.
- Preserve relevant evidence only where safe, lawful and necessary.
- Do not promise confidentiality.
- The DSL will consider parents/carers, children's social care, police, Prevent/Channel or other agencies as appropriate.
- Where the concern relates to a member of staff, follow the school's allegations/low-level concerns procedures and KCSIE.
- Consider whether filtering, monitoring, supervision, curriculum or risk assessments require adjustment following the incident.

13.0 STAFF USE OF TECHNOLOGY AND PROFESSIONAL CONDUCT

Staff use of technology must comply with the Staff Code of Conduct, safeguarding, data protection and acceptable-use expectations. Staff must maintain professional boundaries, protect confidential information and avoid any online behaviour that could compromise pupils, the school or their professional role.

- Do not use personal social-media accounts to communicate privately with pupils.
- Do not photograph or record pupils on personal devices unless expressly authorised under a documented school process.
- Do not share pupil information through unapproved applications or personal cloud storage.
- Immediately report accidental access to illegal or seriously harmful content, security incidents or suspected data breaches.
- Use strong authentication and follow school cyber-security instructions.

14.0 REMOTE AND ONLINE LEARNING

Where remote or online learning is used, the school will ensure appropriate safeguarding, privacy and professional-boundary arrangements. Parents/carers will be informed about relevant platforms and expectations. Staff will use approved accounts and platforms, and any live interaction will be managed in a manner appropriate to pupil age, need and safeguarding risk.

15.0 SEND, EAL AND VULNERABLE PUPILS

Everything Education School recognises that some pupils may face additional online risks or barriers to recognising, understanding or reporting harm. Online safety teaching, supervision and reporting routes will therefore be adapted where necessary for SEND, communication needs, EAL, cognition, sensory needs, social understanding or emotional regulation.

Reasonable adjustments may include visual explanations, simplified language, repetition, explicit teaching of online boundaries, supported reporting, additional supervision and personalised risk management. A pupil's vulnerability will not be used as a reason to exclude them unnecessarily from beneficial technology.

16.0 DATA PROTECTION, PRIVACY AND CYBER SECURITY

Online safety, data protection and cyber security are closely connected. Personal data will be processed lawfully and proportionately. Where monitoring technologies process personal data, the school will consider transparency, privacy information and data protection impact assessment requirements.

- Security incidents and suspected data breaches must be reported promptly.
- Access to personal information will be limited according to role.
- School information must be stored and shared using approved systems.
- Backups, updates, account security and other technical controls will be maintained in line with the school's cyber-security arrangements.
- Third-party educational technology will be considered for safeguarding, privacy, security and contractual suitability before adoption.

17.0 PARENTS, CARERS AND PARTNERSHIP WORKING

The school will work constructively with parents and carers to promote safe technology use. Parents/carers will be made aware, where appropriate, of the online services pupils are expected to use and the school's expectations. Where an online safeguarding concern arises, information will be shared with parents/carers unless doing so would place a child at increased risk or conflict with safeguarding advice.

18.0 TRAINING, MONITORING AND REVIEW

- Online safety forms part of safeguarding induction and ongoing staff training.
- Relevant staff will understand filtering and monitoring arrangements and escalation routes.
- The DSL, senior leadership and IT support will contribute to the annual filtering and monitoring review.
- The school will consider patterns in incidents, pupil voice, staff feedback and technical reports.
- This policy will be reviewed at least annually and sooner following significant incidents, changes in technology, changes in statutory guidance or material changes to the school's systems.

RELATED POLICIES

- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Anti-Bullying Policy
- Behaviour Policy
- Data Management / Data Protection Policy
- SEND Policy

- Equality, Diversity and Inclusion Policy
- Curriculum and PSHE/RSHE arrangements
- Whistleblowing Policy
- Allegations Against Staff / Low-Level Concerns procedures
- Lockdown and Evacuation Policy
- Health and Safety Policy
- Acceptable Use arrangements and relevant privacy notices

APPENDIX 1 - ONLINE SAFETY INCIDENT RESPONSE CHECKLIST

- Is anyone in immediate danger? If yes, take urgent protective action and contact emergency services where necessary.
- Inform the DSL/DDSL promptly.
- Record what was seen, heard or reported factually.
- Do not conduct an unnecessary investigation or repeatedly question the pupil.
- Do not forward, copy or routinely view illegal or sexual imagery.
- Secure devices/evidence only where this can be done safely and lawfully.
- Consider whether parents/carers and external agencies should be informed.
- Record decisions, actions and outcomes.
- Review any required changes to risk assessment, supervision, filtering/monitoring or curriculum.

APPENDIX 2 - FILTERING AND MONITORING REVIEW CHECKLIST

- Named senior leader, DSL and technical responsibilities confirmed.
- Current pupil risk profile considered, including SEND and EAL.
- School-managed devices and relevant locations/connection types checked.
- Filtering categories, blocklists and safe-search arrangements reviewed.
- Monitoring methods, alert thresholds and escalation routes reviewed.
- Generative AI and dynamic/personalised content risks considered.
- Remote/off-site device use considered.
- Guest/BYOD access considered where applicable.
- Sample checks completed to confirm controls operate as intended.
- Staff awareness and classroom supervision reviewed.
- Incidents and monitoring reports reviewed for patterns.
- Temporary exceptions and approvals reviewed.
- Actions, owners and completion dates recorded.
- Outcome reported to proprietor and retained for inspection/assurance.

REFERENCE SOURCES

Department for Education, Keeping Children Safe in Education 2026 (in force from 1 September 2026).

Department for Education, Meeting digital and technology standards in schools and colleges - Filtering and monitoring: core standard (updated 16 September 2026).

Department for Education, Data protection in schools guidance (updated 9 July 2026).