

Madeley Academy



Online Safety Policy

Prepared by:	Neil Davies / Ian Marshall
Date:	September 2026
Approved by LGB date:	July 2026
Review Date:	September 2027

Contents

Statement of Intent and Safeguarding Culture
Scope and Definitions of the Policy
Statutory and Non-Statutory Framework
Policy Development, Monitoring and Review
Roles, Responsibilities, Governance and Accountability
Online Safety Risk Assessment and Evidence Base
Filtering and Monitoring
Online Safety Curriculum, RSHE and Sixth Form Provision
The Four Cs of Online Risk
Artificial Intelligence, Generative AI, and Deepfakes
Policy Statements
Mobile Phones, BYOD and Wearable Technology
Use of Digital and Video Images
Remote Learning and Approved Platforms
Vulnerable Learners and Contextual Safeguarding
Sixth Form and Post-16 Provision
Data protection, confidentiality, and cyber security
Reporting, Recording and Responding to Incident
Illegal Content, Extremism and Cybercrime
Sources of support and advice
Appendices

Statement of Intent and Safeguarding Culture

Madeley Academy recognises that online safety is not a technical add-on; it is a core safeguarding and child protection responsibility.

The Academy will protect students from harm online and offline, teach them to understand and manage risk, and respond quickly and proportionately when concerns arise.

This policy supports a whole-school approach in which online safety is embedded in safeguarding, behaviour, attendance, curriculum, pastoral care, staff conduct, data protection, IT governance and sixth form provision.

The Academy recognises that children and young people move seamlessly between online and offline environments and that online harms may occur on school systems, personal devices, third-party platforms, gaming environments, social media, messaging apps, AI tools and home networks.

- Online safety concerns will be treated as safeguarding concerns where they involve risk of harm, exploitation, abuse, harassment, criminality, radicalisation, mental health impact, coercion, image-based abuse, grooming, bullying, harmful sexual behaviour or misuse of personal data.
- All staff have a responsibility to identify, report and respond to online safety concerns in line with safeguarding procedures. Online safety is not solely a technical function but a whole-school safeguarding duty.

The Academy will maintain a culture in which students, including sixth form students, know how to seek help and are confident that concerns will be taken seriously.

The Academy will balance protective filtering and monitoring with education that develops resilience, digital literacy, critical thinking and respectful online conduct.

- Leaders will be able to evidence how online safety is taught, monitored, reviewed and improved.

Scope and Definitions of the Policy

This policy applies to all members of the Academy community, including students in Years 7–13, staff, governors, trustees, volunteers, contractors, visitors, parents/carers and community users who access Academy systems, networks, devices, platforms or data, whether on site or remotely.

For the purposes of this policy, online safety includes the safe, responsible and lawful use of technology, digital systems, internet-connected devices, social media, online services, artificial intelligence, generative AI, cloud platforms, digital communications, personal devices and Academy-owned devices.

The Academy may respond to online incidents that occur away from the Academy site where the incident is linked to membership of the Academy, affects the safety or welfare of a student or staff member, impacts learning, involves Academy systems, or brings the Academy into disrepute.

Responses will be consistent with the Behaviour Policy, Anti-Bullying Policy, Safeguarding and Child Protection Policy, Staff Code of Conduct and relevant statutory guidance.

Under the Education and Inspections Act 2006, the Headteacher has the power, to such extent as is reasonable, to regulate the behaviour of students when they are off-site, and staff may impose disciplinary sanctions for inappropriate behaviour in accordance with the Academy's published Behaviour Policy.

These powers are particularly relevant to incidents of cyber-bullying and other online safety concerns that occur outside the Academy but are connected to the Academy community.

The Education Act 2011 further strengthened these powers by extending staff authority to search electronic devices and, where permitted by law, delete data. The Academy will respond to such incidents in accordance with the Behaviour Policy, Anti-Bullying Policy, Safeguarding and Child Protection Policy, Staff Code of Conduct and relevant statutory guidance.

Where appropriate, parents/carers will be informed of incidents of inappropriate online behaviour that occur outside the Academy.

Statutory and Non-Statutory Framework

This policy aligns with Keeping Children Safe in Education (KCSIE), including expectations relating to online safety, the Four Cs framework (content, contact, conduct, commerce), filtering and monitoring requirements, and safeguarding responsibilities for all staff.

Regard has been given to **Keeping Children Safe in Education 2026 Annex C: Online Safety**, including leadership responsibilities, filtering and monitoring requirements, staff training expectations, safeguarding responses and the education of children in safe online behaviours.

The policy should be read alongside the Academy Safeguarding and Child Protection Policy, Behaviour Policy, Anti-Bullying Policy, Staff Code of Conduct, Data Protection Policy, Privacy Notices, IT Acceptable Use Agreements, Special Educational Needs and Disabilities Policy, RSHE Policy, Whistleblowing Policy, Low-Level Concerns Policy, Cyber Security arrangements and Trust/MAT digital standards.

The policy is informed by, and should be reviewed against, the following current and emerging requirements:

- This policy has been reviewed against Keeping Children Safe in Education 2026 and will be updated further should additional statutory guidance be issued.
- Working Together to Safeguard Children.
- DfE Meeting digital and technology standards in schools and colleges, including the filtering and monitoring core standard and cyber security standard.
- The Online Safety Act 2023 and Ofcom implementation of illegal content and child safety duties for regulated online services.
- The Academy will monitor developments in Ofcom guidance and Online Safety Act implementation to ensure that safeguarding procedures, curriculum provision and risk assessments remain responsive to emerging online harms and technological developments.
- DfE Teaching online safety in schools' guidance and statutory RSHE / relationships, sex and health education requirements.
- Education for a Connected World framework and UKCIS / UK Safer Internet Centre guidance on appropriate filtering and monitoring.
- Prevent Duty guidance and responsibilities to protect students from extremist and terrorist material online.
- UK GDPR, Data Protection Act 2018, Computer Misuse Act 1990, Protection of Children Act 1978, Sexual Offences Act 2003, Malicious Communications Act 1988, Communications Act 2003, Public Order Act 1986, Obscene Publications legislation, Voyeurism (Offences) Act 2019 and relevant image-based abuse legislation.

Policy Development, Monitoring and Review

This Policy has been developed by the Online Safety Group, which is made up of:

- Headteacher/senior leaders
- DSL
- Online Safety lead
- Staff – including teachers/support staff/technical staff
- Governors

Schedule for Development, Monitoring & Review

The implementation of this policy will be monitored by the:	D Marshall –DSL / Safeguarding N Davies – DDSL / Online Safety Lead I Marshall – ICT Lead / Online Safety Coordinator M Powell – MIS Services Manager Layton Chantry – IT Infrastructure Services Manager Pauline Hughes – Link Governor
Monitoring will take place at regular intervals:	Termly
The Governing Board will receive a report on the implementation of the policy generated by the monitoring group (which will include anonymous details of Online Safety incidents) at regular intervals:	Termly
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online Safety or incidents that have taken place. The next anticipated review date will be:	July each year for publication in the Autumn Term or as developments dictate earlier revision
Should serious Online Safety incidents take place, the following external persons/agencies should be informed:	LA Safeguarding Officer, Police

The Academy will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys/questionnaires of:
 - a) students
 - b) parents/carers
 - c) staff

Leaders evaluate the impact of online safety provision through analysis of incident trends, student voice, staff confidence and safeguarding outcomes. Findings inform strategic improvements and curriculum development.

Monitoring Evidence and Assurance

To evidence compliance with statutory safeguarding requirements, KCSIE, DfE Filtering and Monitoring Standards, and the Online Safety Act, the DSL, Deputy DSLs, Online Safety Lead and Online Safety Coordinator will maintain and review a range of monitoring information including:

- Smooth wall Filtering and Monitoring reports;
- Filtering review records
- Online safety incident records and safeguarding trends recorded on CPOMS;
- Student voice surveys and pupil feedback;
- Staff training records;
- Parent and carer engagement activities, communications and feedback;
- Governor monitoring visits;
- Online Safety Group meeting minutes and actions;
- Curriculum monitoring;
- Annual risk assessments;

This evidence will be used to evaluate the effectiveness of the Academy's online safety provision, identify emerging risks, inform curriculum development, support safeguarding practice and provide assurance to governors and trust leaders.

Roles and Responsibilities	Governors Headteacher and Senior Leaders Online Safety Lead Online Safety Co-ordinator Technical Staff/ MIS Services Manager/ IT Infrastructure Services Manager Teaching and Support Staff Child Protection/Safeguarding Designated Person Online Safety Committee Students Parents/Carers
Policy Statements	Education – Students Education – Parents/Carers Education and training – Staff/Volunteers Training – Governors Technical – infrastructure/equipment, filtering and monitoring Bring your own devices (BYOD) Use of digital and video images Data protection Communications User Actions – unsuitable/inappropriate activities
Appendices	Acceptable Use Policy – Staff Acceptable Use Policy – Students Responding to incidents of misuse – flowchart Actions and Sanctions Smoothwall Cloud Filter Smoothwall Monitor

Roles, Responsibilities, Governance, Leadership and Accountability

The following section outlines the Online Safety roles and responsibilities of individuals and groups within the Academy:

Governors: Pauline Hughes

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about Online Safety incidents and monitoring reports. Pauline Hughes, a member of the Governing Board has taken on the role of Online Safety Governor.

The role of the Online Safety Governor will include:

- Regular meetings with the Online Safety Lead / Coordinator
- Regular monitoring of Online Safety incident logs
- Regular monitoring of filtering/change control logs
- Reporting to Governing Board

Headteacher and Senior Leaders

The Headteacher has a duty of care for ensuring the safety (including Online Safety) of members of the Academy community, though the day-to-day responsibility for Online Safety will be delegated to the DSL, Online Safety Lead and Online Safety Co-ordinator.

The Designated Safeguarding Lead (DSL) holds overall responsibility for online safety. An appointed Online Safety Lead supports the implementation of filtering, monitoring, curriculum delivery and staff training.

The Headteacher and another member of the Senior Leadership Team will be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff (see flow chart on dealing with Online Safety).

The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Coordinator and Lead and other relevant staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.

- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in the Academy who carry out the internal Online Safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator and Lead

Online Safety Lead and Coordinator

Neil Davies, Online Safety Lead / DDSL (under the direction of the DSL) has a day-to-day responsibility for Online Safety within the Academy and is supported by the Online Safety Coordinator (I Marshall). He:

- Leads the Online Safety committee
- Takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the Academy's Online Safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place
- Provides training and advice for staff
- Liaises with the Local Authority where appropriate
- Liaises with Academy technical staff, receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments,
- Meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- Attends relevant meetings of Governors
- Reports to Senior Leadership Team
- Follows the Safeguarding Policy and passes on concerns to the DSL

IT Services/Technical Staff

IT Technical staff are responsible for ensuring:

- That the Academy's technical infrastructure is secure and is not open to misuse or malicious attack
- That the Academy meets required Online Safety technical requirements and any Local Authority Online Safety policy/guidance which may apply
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- The filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- That they keep up to date with Online Safety technical information to effectively carry out their Online Safety role and to inform and update others as relevant
- That the use of the network/internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Senior Leader/Online Safety Lead / Coordinator for investigation/action/sanction
- That monitoring software/systems are implemented kept up to date
- Follows the Safeguarding Policy and passes on concerns to the DSL
- The implementation, enforcement and ongoing support of trust wide digital policies and standards

Teaching and Support Staff

All other staff are responsible for ensuring that:

- They have an up-to-date awareness of Online Safety matters and of the current Academy Online Safety policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy/Agreement (AUP)
- They report any suspected misuse or problem to the Headteacher/Senior Leader/Online Safety Lead / Coordinator for investigation/action/sanction
- All digital communications with students/parents/carers should be on a professional level and only carried out using official Academy systems
- Online Safety issues are embedded in all aspects of the curriculum and other activities
- Students understand and follow the Online Safety and acceptable use policies
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other Academy activities (where allowed) and implement current policies regarding these devices
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Follows the Safeguarding Policy and passes on concerns to the DSL

Child Protection/Safeguarding Designated Person/Officer / DSL

The Academy Child Protection/Safeguarding Designated Officer is D Marshall (Senior Deputy Head) and is trained in Online Safety issues and aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

It is important to emphasise that these are child protection issues, not technical issues simply that the technology provides additional means for child protection issues to develop.

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the Academy community, with responsibility for issues regarding Online Safety and the monitoring of the Online Safety policy including the impact of initiatives. The group will be responsible for regular reporting to the Governing Body/Directors.

Members of the Online Safety Group will assist the Online Safety Lead / Coordinator with:

- The production/review/monitoring of the Academy Online Safety policy/documents
- The production/review/monitoring of the Academy filtering policy and requests for filtering changes
- Mapping and reviewing the Online Safety curricular provision – ensuring relevance, breadth and progression
- Monitoring network/internet/incident logs
- Consulting stakeholders – including parents/carers and the students about the Online Safety provision
- Monitoring improvement actions identified through use of the 360-degree safe self-review tool

Students / Learners

- Are responsible for using the Academy digital technology systems in accordance with the Student Acceptable Use Policy
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know the rules on the use of mobile devices and digital cameras. They should also be aware of the risks of taking/use of images and cyber-bullying.
- Should understand the importance of adopting good Online Safety practice when using digital technologies out of the Academy and realise that the Academy's Online Safety Policy covers their actions out of the Academy, if related to their membership of the Academy

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Parents/carers will be encouraged to support the Academy in promoting good Online Safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at Academy events
- Access to parents' sections of the website/VLE and on-line student records
- Their children's personal devices in the Academy (where this is allowed)

Online Safety Risk Assessment and Evidence Base

The Academy will maintain an online safety risk assessment that reflects its context as a secondary school with sixth form. The assessment will consider technology use, curriculum, student age, SEND, EAL, disadvantage, looked-after and previously looked-after children, students with social workers, mental health need, harmful sexual behaviour, image-based abuse, cyberbullying, AI risks, cybercrime, radicalisation, online exploitation and local safeguarding intelligence.

- Risk assessment will be reviewed at least annually and following significant incidents or technology changes.
- Findings will inform filtering settings, monitoring strategy, curriculum planning, staff training and parental communication.
- Leaders will retain evidence of decisions, including where access is allowed for educational reasons and how risks are mitigated.
- Evidence retained may include filtering review documentation, monitoring reports, safeguarding records, curriculum reviews, training records, student voice findings, governor monitoring reports and risk assessment updates. This evidence will support quality assurance and external inspection processes.

Using the Four Cs in Risk Assessment

When undertaking online safety risk assessments, leaders will consider potential risks under each of the Four Cs framework and identify appropriate control measures, including:

- Filtering and monitoring arrangements.
- Curriculum interventions.
- Targeted support for vulnerable learners.
- Staff training requirements.
- Parent/carer information and guidance.
- Multi-agency safeguarding responses where appropriate.

Filtering and Monitoring

Statement of Intent

The Academy will provide a safe and secure online environment through effective filtering and monitoring systems delivered via Smoothwall, as part of its safeguarding responsibilities in line with *Keeping Children Safe in Education*, DfE filtering and monitoring standards, and the Online Safety Act.

Filtering is preventative and limits access to illegal, inappropriate and harmful content. Monitoring is reactive and identifies safeguarding risks and concerns. These systems form part of a wider safeguarding strategy that includes education, supervision and acceptable use.

Filtering and monitoring are understood by leaders, DSLs, governors, IT Services and all staff, and are subject to regular review and oversight.

Infrastructure, Systems and Technical Security

The Academy is responsible for ensuring that its infrastructure and network are as safe and secure as is reasonably possible.

- Technical systems are managed in line with recommended DfE standards and cyber security expectations
- Regular reviews and audits of safety and security are undertaken
- Servers, wireless systems and cabling are securely located with restricted access
- All users have clearly defined access rights
- All users are provided with a secure username and password and are responsible for maintaining their security
- Administrator passwords are securely stored and accessible to the Headteacher or nominated senior leader
- Up-to-date anti-virus and endpoint protection are in place across all devices
- Software licensing is monitored and maintained accurately

Appropriate security measures protect systems, including servers, firewalls, routers, devices and cloud systems, from accidental or malicious compromise.

Filtering Provision (Smoothwall Cloud Filter)

The Academy uses Smoothwall Cloud Filter as its primary filtering system across all devices and networks.

- Smoothwall filtering is deployed across:
 - Windows, Chromebooks, macOS, iOS and Android devices
- Filtering operates via a cloud-based client installed on managed devices, which:
 - Applies filtering policies directly to devices
 - Filters internet traffic locally on the device
 - Provides protection both on-site and off-site

The system enables:

- Dynamic web and application filtering
- SSL inspection without requiring intrusive decryption methods
- User-level identification through logged-in accounts
- Filtering coverage includes:
 - Fully identified dynamic filtering on managed devices
 - DNS-based filtering on unmanaged devices where applicable

Filtering will:

- Block illegal content, including child sexual abuse material using recognised block lists
- Prevent access to harmful or inappropriate material, including:
 - Extremism, terrorism and radicalisation
 - Pornography and sexual content
 - Self-harm, suicide and eating disorder content
 - Bullying, hate and violence
 - Criminal activity, substances and gambling
- Be age-appropriate and differentiated, including:
 - Lower school students
 - Sixth form learners
 - Staff and administrative access
 - SEND and vulnerable learners
- Include safe search and restricted modes where appropriate

The Academy will take reasonable steps to prevent circumvention of filtering through VPNs, proxies, anonymisers, private DNS and unauthorised applications.

The Academy recognises that filtering cannot provide a 100% guarantee of protection, due to the dynamic nature of online content.

Monitoring Provision (Smoothwall Monitor)

The Academy uses **Smoothwall Monitor** to provide proactive, real-time monitoring of user activity.

- Smoothwall Monitor provides:
 - **Real-time monitoring of user activity**, including keystroke capture across applications and platforms
 - Continuous safeguarding oversight supported by a **24/7/365 human moderation team**
- Monitoring identifies:
 - Harmful or concerning searches
 - Bullying, harassment or harmful communications
 - Indicators of self-harm or mental health concerns
 - Extremism, exploitation or sexual harm
 - Cybercrime or misuse of systems

- Monitoring operates:
 - At operating system level on Windows devices (full coverage across applications)
 - Through user-linked extensions on Chromebooks
 - Through controlled browser environments on iPads and managed devices
- Alerts are:
 - Automatically generated and analysed
 - Reviewed and validated by **trained safeguarding professionals**
 - Prioritised to reduce false positives
 - Escalated to the Academy for action as appropriate

Users are made aware of monitoring through the Acceptable Use Agreement.

Roles and Responsibilities

- Governors: Provide assurance that filtering and monitoring are effective
- Headteacher/Senior Leaders: Ensure systems are implemented and reviewed
- DSL/Deputy DSLs: Lead safeguarding response to alerts
- Online Safety Lead: Coordinates implementation and review
- IT Services: Maintain systems and technical controls
- All Staff: Follow procedures and report concerns

Review and Testing

Filtering and monitoring are formally reviewed at least annually, and more frequently where there are significant changes.

The annual review will be undertaken by the DSL, Online Safety Lead and IT Infrastructure Services Manager and Online Safety Governor. The review will be documented and will consider DfE Filtering and Monitoring Standards, safeguarding trends, emerging technologies, user feedback and any recommendations arising from incidents or audits. Evidence of the review will be retained and reported to the Local Governing Board.

Review includes:

- Effectiveness of filtering and monitoring systems
- Alert data, response times and accuracy
- Risks relating to vulnerable groups and sixth form learners
- Impact of emerging technologies, including AI
- Staff confidence and training needs

Technical testing is recorded, and filtering changes are:

- Logged and risk-assessed
- Approved by designated staff
- Time-limited where appropriate

Outcomes are reported to the Local Governing Board.

Reporting and Responding to Concerns

Where concerns are identified:

1. Alerts or concerns are identified via Smoothwall systems, staff observation or reporting
2. Designated staff triage the concern
3. Safeguarding concerns are escalated immediately to the DSL
4. Concerns are recorded on the safeguarding system
5. Behavioural and technical concerns are managed appropriately

Where illegal material is suspected, staff must not view, copy or share the material and must follow safeguarding procedures.

Additional Safeguards and Acceptable Use

The Academy maintains policies for:

- Guest access to systems
- Personal use of Academy devices
- Installation of software (restricted)
- Use of removable media

Personal data must not be removed from site unless securely encrypted.

The Academy assesses risks associated with:

- Mobile devices and BYOD
- Cloud services and remote learning
- Artificial intelligence and emerging technologies

Sixth Form Provision

The Academy recognises the need for a balanced approach for sixth form learners:

- Filtering is adjusted to support independent research and study
- Monitoring remains active to identify safeguarding risks
- Students are supported to develop digital resilience and safe online behaviours
-

Online Safety Curriculum, RSHE and Sixth Form Provision

The Academy will provide a planned, sequenced and age-appropriate online safety curriculum through Computing, PSHE/RSHE, assemblies, tutor time, subject teaching and sixth form personal development. The curriculum will support students to understand online risks, recognise harmful behaviour, seek help and use technology safely, responsibly and respectfully.

- Online relationships, consent, boundaries, digital reputation and respectful communication.
- Cyberbullying, harassment, misogyny, hate, discrimination and harmful online challenges.
- Image sharing, nude and semi-nude images, image-based abuse, deepfakes and manipulated media.
- Grooming, exploitation, coercion, financial exploitation, sextortion and online radicalisation.

- Misinformation, disinformation, extremism, conspiracy content and critical evaluation of online information.
- Privacy, personal data, location sharing, passwords, phishing, scams and cyber security.
- AI literacy, generative AI limitations, bias, hallucination, academic integrity, deepfakes and safe prompting.
- Where to get help, including trusted adults, DSL team, CEOP, Childline, Report Harmful Content and platform reporting tools.

Curriculum provision will be adapted for students with SEND, EAL, additional vulnerabilities and differing levels of maturity. Sixth form provision will explicitly address adult-facing platforms, age assurance, adult content, online gambling, financial scams, digital footprint, employment and university admissions, consent, intimate image abuse, AI use in coursework, professional communication and independent living online safety.

The Four Cs of Online Risk

The Academy uses the UK Council for Internet Safety (UKCIS) Four Cs Framework, recognised within Keeping Children Safe in Education, to help identify, assess and respond to online risks experienced by children and young people.

Online risks can be categorised as:

Risk Category	Examples
Content	Exposure to harmful, inappropriate or illegal content, including pornography, extremist material, self-harm or suicide content, misinformation, disinformation and harmful online challenges.
Contact	Harm arising through interaction with others online, including grooming, exploitation, radicalisation, coercion, fraud, unwanted contact and online predators.
Conduct	Behaviour by an individual online that negatively affects themselves or others, including cyberbullying, harassment, hate speech, sharing of harmful content, image-based abuse and inappropriate use of social media or AI-generated content.
Commerce	Risks associated with online financial activity, including scams, phishing, gambling, loot boxes, in-app purchases, fraud, financial exploitation and misuse of personal data.

The Academy recognises that online harms often overlap across multiple categories and may present as safeguarding concerns requiring intervention by the Designated Safeguarding Lead (DSL) and safeguarding team.

The Four Cs framework informs:

- Curriculum planning and delivery.
- Filtering and monitoring decisions.
- Safeguarding risk assessments.
- Staff training.
- Student education and awareness.
- Parent and carer engagement.
- Responses to online safety incidents.

Age-appropriate examples of each of the Four Cs are taught throughout Years 7–13 through Computing, PSHE/RSHE, tutor programmes, assemblies and pastoral activities, with additional adaptations made for vulnerable learners, students with SEND and sixth form students.

Artificial Intelligence, Generative AI and Deepfakes

The Academy recognises both the educational opportunities and safeguarding risks associated with artificial intelligence. AI tools may generate text, images, audio, video or personalised content. Risks include inaccurate information, bias, harmful advice, age-inappropriate content, grooming, deepfakes, impersonation, sexualised or abusive image manipulation, academic misconduct, privacy breaches, cybercrime and over-reliance.

- Students may only use AI tools in line with Academy guidance, teacher instructions and assessment rules.
- Staff must risk assess AI tools before use with students, considering age suitability, data protection, terms of use, moderation, record keeping and safeguarding risks.
- No personal, sensitive or safeguarding information about students, staff or families may be entered into public AI tools unless explicitly approved through the Academy's data protection and safeguarding procedures.
- AI-generated or manipulated images, audio or video used to humiliate, harass, impersonate, abuse, sexualise or coerce another person will be treated as a serious safeguarding and behaviour matter and may be referred to external agencies.
- Leaders will consider the capability of filtering and monitoring systems to identify AI-generated and dynamic content and will record any limitations and mitigations.
- Concerns regarding staff use of technology, artificial intelligence, social media, online conduct or professional boundaries will be managed in accordance with the Staff Code of Conduct, Safeguarding and Child Protection Policy, Allegations Procedures and Low-Level Concerns Policy.

Policy Statements

Education - Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in Online Safety is therefore an essential part of the Academy's Online Safety provision. Children and young people need the help and support of the Academy to recognise and avoid Online Safety risks and build their resilience.

Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages across the curriculum. The Online Safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and will be provided in the following ways:

- A planned Online Safety curriculum will be provided as part of Computing/PHSE/other lessons and should be regularly revisited
- Key Online Safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students will be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information

- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students will be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside the Academy
- Staff will act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students will be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need

Education – Parents/Carers

Many parents/carers have only a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours. Parents can underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The Academy will therefore seek to provide information and awareness to parents/carers through:

- Curriculum activities
- Letters, newsletters, web site
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications

Education & Training – Staff

It is essential that all staff are aware of Online Safety and understand their responsibilities, as outlined in this policy:

- All staff receive online safety and safeguarding training at induction, with updates provided at least annually, in line with KCSIE expectations.
- All new staff should receive Online Safety policies as part of their induction programme, ensuring that they fully understand the Academy's Online Safety policy and Acceptable Use Agreements
- The Online Safety Lead / Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations
- This Online Safety policy and its updates will be presented to staff in staff/team meetings/INSET days
- The Online Safety Lead / Coordinator will provide advice/guidance/training to individuals as required

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. However, there are a number of Online Safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive, and a BYOD policy should be in place and reference made within all relevant policies.

- The Academy has a set of clear expectations and responsibilities for all users
- The Academy adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the Academy's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the Academy will follow the process outlined within the BYOD policy

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The Academy will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- Staff will use Academy-approved equipment and platforms for images, recording, and publication.
- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at Academy events for their own personal use (as such use is not covered by the Data Protection Act). To respect privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images

- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow Academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Academy equipment; the personal equipment of staff should not be used for such purposes including removal of Meta Data and the use of low-resolution images
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the Academy into disrepute
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images
- Livestreaming or recording lessons/events must be authorised and risk assessed.

Remote Learning and Approved Platforms

Madeley Academy is committed to providing a safe environment for online learning. This commitment remains the same in the difficult circumstances brought about during any period of remote or blended learning.

During any period of Guided Home Learning our expectations of staff and pupils also remain the same, and the principles and practices of the Academy's *Safeguarding and Child Protection Policy* and *Online Safety Policy*, staff Code of Conduct and *Acceptable Use Agreements* for staff and pupils will continue to apply, both to existing and any new online and distance learning arrangements introduced. Staff and pupils must review these policies and ensure that they always adhere to them.

Given any changes in circumstances to everyday teaching and learning practices, the following guidelines will also apply:

Providing a safe system

- Where the site remains open, the Academy will continue to ensure that appropriate filters and monitoring systems are in place to protect children when they are online on the Academy's IT systems or recommended resources.
- For the purposes of guided home learning, the primary platforms used across the Academy network are:
 - Microsoft Teams
 - Socrative
 - Educake
 - Maths Watch
 - My Maths

The Academy has central oversight of and can monitor activity and communications through these platforms. The platforms are restricted to Academy users only and permissioned accordingly. Other platforms may be used at times for specific purposes. The online safety implications of any platform are carefully considered before use.

- The Academy network both have technical support dedicated to maintaining a safe and operational online environment.
- The Academy's Designated Safeguarding Lead (DSL) and Online Safety Lead has day to day responsibility for online safety and will maintain an active oversight of the management of guided home learning from a safeguarding perspective. Procedures will be kept under review, and action will be taken swiftly if concerns about the use of technologies arise.
- The Academy will keep in regular contact with parents, updating them as appropriate with information on how the Academy is providing guided home learning, how they can keep their children safe online, and any new developments.

Guided Home Learning

There is a wide range of formats for guided home learning, including:

- Posting activities for students at regular intervals, with student responses
- Directing students to web-based resources and activities they can engage with on or offline.

Teachers will provide a variety of learning experiences within a lesson, across the Academy Day/week and through a scheme of work.

Protocols for Staff in Relation to Guided Home Learning:

- Only use Academy approved platforms; do not use social media in communicating with students
- Reinforce online safety messages regularly in your teaching
- Bear in mind the current circumstances and how they are affecting students and families when setting expectations
- Consider online safety when sharing resources – vet websites and videos/apps/software carefully and bear in mind that the home environment will not have the same content filtering systems as at the Academy. If introducing new apps and resources, ensure these meet GDPR requirements. Contact your line manager / network manager for further guidance.
- If concerned about online safety/resources, check with IT support/digital leader
- Ensure that passwords and secure information – such as logins for Bromcom – are kept confidential
- Adhere to copyright and GDPR guidelines
- Continue to look out for signs that a student may be at risk – which may differ from typical triggers in the Academy environment. Report any concerns to the DSL without delay in the usual way
- Do not provide students or parents with personal contact details – email, home or mobile numbers, details of web-based identities etc.
- Do not arrange to meet students or ask them to deliver work to your home
- Remain professional and objective in all email and other forms of correspondence
- Any child protection or safeguarding concern must be reported to the DSL without delay

Reporting an issue for staff:

- Concerns about the safety of procedures, behaviours or use of technology should be referred to the DSL
- Routine queries about the use of apps or online materials should be addressed to your line manager or IT support depending on the nature of the issue
- UKSICs Professionals Online Safety Helpline is a good source of external advice **Protocols for students in relation to guided home learning:**
- Always log on through your Academy account and use your Academy email for Academy business
- Do not make recordings, take screenshots/screengrabs or photographs, or store footage of teachers or other students
- If you have concerns about online safety, or if you feel you are being bullied, talk to someone you trust

Vulnerable Learners and Contextual Safeguarding

The Academy recognises that some students may be more vulnerable to online harm due to SEND, communication needs, previous abuse, isolation, mental health, social care involvement, care experience, disadvantage, EAL, bereavement, identity-based bullying, exploitation, attendance issues or other contextual factors. Online safety support will be personalised and will not rely solely on generic messages.

- Risk assessments and support plans will consider online activity and potential vulnerability.
- Curriculum materials will be adapted to meet learning, language and maturity needs.
- The DSL team will consider whether online incidents indicate wider safeguarding concerns.
- Pastoral and sixth form teams will work with parents/carers and external agencies where appropriate.

Sixth Form and Post-16 Provision

Sixth form students require distinct online safety provision reflecting greater independence, adult-facing platforms, employment, driving, relationships, finance, university preparation and increased use of personal devices. The Academy will maintain high expectations while preparing students for safe adult participation online.

- Post-16 students will be taught about digital reputation, employment screening, university admissions, online professionalism and consent.
- Provision will cover online pornography, age assurance, intimate image abuse, coercion, sextortion, domestic abuse in young adult relationships, gambling, trading scams, cryptocurrency scams, misinformation, extremism and online radicalisation.
- Sixth form students will receive guidance on lawful and ethical AI use, referencing, academic integrity and assessment malpractice.
- Provision will also include awareness of age assurance systems, emerging online platforms, online financial risks, digital identity verification, employment-related cyber security risks and safe participation in adult online environments.

- Sixth form leadership will monitor online safety trends and support students affected by online harms.

Data protection, Confidentiality and Cyber Security

Online safety depends on effective data protection and cyber security. The Academy will manage personal data lawfully, securely and transparently. Staff and students must protect credentials and report suspected breaches, phishing, malware, unauthorised access or lost devices immediately.

- Passwords must not be shared. Multi-factor authentication will be used where required or available.
- Access rights will be role-based, reviewed and removed promptly when users leave or change role.
- Personal data must not be uploaded to unapproved apps, AI tools or cloud services.
- Sensitive data transferred outside secure systems must be encrypted or otherwise protected.
- Technical controls will include secure configuration, updates, malware protection, backups, firewall/security controls, audit logs and incident response processes.

Reporting an issue

Online safety concerns are recorded on the Academy's safeguarding system (CPOMS) and reviewed by the DSL team.

For students:

- Speak to a trusted adult
 - Email your tutor
 - Contact Childline 0800 1111 or CEOP
- #### **The role of parents**
- It is the responsibility of parents to ensure that pupils are monitored in their use of technology for guided home learning as they would ordinarily do when their children are using technology at home. Monitoring screen time is particularly important in the current circumstances
 - While students are working from home, they are connected to their home broadband so their traffic doesn't go through the Academy firewall – parents will therefore need to ensure that age-appropriate filtering or safe search is enabled at home. Information on setting this up can be found at: <https://saferinternet.org.uk/> and here: <https://www.internetmatters.org/parental-controls/>
 - Communication during online learning is between student and teacher: parents should communicate with Academy/staff in the usual manner, via Academy email or telephone during a period of guided home learning
 - Any parent wishing to supplement the Academy's guided home learning with support from online companies or individual tutors should be mindful of the importance of using reputable organisations or individuals who can provide evidence that they are safe and can be trusted to have access to children – further information can be found in the sources of support below
 - Social media, networking apps and gaming platforms are particularly popular now. Parents are advised to be mindful of age restrictions and to oversee their child's social media activity

- The Academy will update parents regularly on online safety matters. Parents are requested to heed the Academy's advice and contact the Academy if they have concerns or encounter risk online
- **Reporting an issue for parents:**
- Contact the DSL for any safeguarding or child protection or online safety concern
- Email the Academy – safeguarding@madeleyacademy.com
- You can also report an incident to CEOP
- <https://www.ceop.police.uk/Safety-Centre/Should-I-make-a-report-to-CEOP-YP/Should-I-make-a-report-to-CEOP-concerned-adult/>
- or Report Harmful Content <https://reportharmfulcontent.com/>
- Contact your child's tutor in the usual way for routine queries about guided home learning
- See the sources of support and advice below

Illegal Content, Extremism and Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer) Children with skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime. If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), will consider referring into the Cyber Choices programme. Our school will meet the required DfE Cyber security standards for schools.

The Academy recognises the duties introduced by the Online Safety Act 2023, including risks associated with user-generated content platforms, illegal content and age-inappropriate material, and ensures that students are educated to recognise and report such risks.

Sources of Support and Advice:

UK Safer Internet Centre <https://www.saferinternet.org.uk/> - includes a range of activities for children of different ages

CEOP / Thinkuknow <https://www.thinkuknow.co.uk/> - includes a range of home activity packs

National Online Safety <https://nationalonlinesafety.com/> - good guides for parents and staff

Parent Info <https://parentinfo.org/> - specifically aimed at parents

Internet Matters <https://www.internetmatters.org/> - specifically aimed at parents

Cyber Choices <https://www.nationalcrimeagency.gov.uk/cyber-choices>

Communications

	Staff & Other Adults				Students			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Communication Technologies								
Mobile phones may be brought to the Academy	✓				✓			
Use of mobile phones in lessons		✓						✓
Use of mobile phones in social time	✓					✓		
Taking photos on mobile phones/cameras		✓						✓
Use of other mobile devices e.g. tablets, gaming devices		✓						✓
Use of personal email addresses in the Academy, or on the Academy network				✗				✗
Use of the Academy email for personal emails				✗				✗
Use of messaging apps		✓						✗
Use of social media			✓					✗
Use of blogs				✗				✗

When using communication technologies, the Academy considers the following as good practice:

- The official Academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students will therefore use only the Academy email service to communicate with others when in the Academy, or on Academy systems (e.g. by remote access)
- Users must immediately report to the nominated person – in accordance with the Academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and students or parents/carers (email, chat, etc) must be professional in tone and content. These communications may only take place on official (monitored) Academy systems. Personal email addresses, text messaging or social media must not be used for these communications
- Students should be taught about Online Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies
- Personal information should not be posted on the Academy website, and only official email addresses should be used to identify members of staff.

Unsuitable/Inappropriate activities

User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Un-acceptable	Un-acceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the Academy or brings the Academy into disrepute				X	

Using Academy systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Academy				X	
Infringing copyright					X
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X
Creating or propagating computer viruses or other harmful files					X
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X			
On-line gaming (non educational)		X			
On-line gambling				X	
On-line shopping / commerce			X		
File sharing		X			
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. YouTube		X			

Appendices

Staff - Acceptable Use Policy Agreement

The aim of this policy is to provide clarification to staff on the use of emerging technologies so that a teacher's professional position is not compromised. It should be read in conjunction with the Child Protection Policy which offers further guidance on safeguarding issues.

I understand that I must use the Academy ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed Online Safety in my work with young people.

For my professional and personal safety:

- I understand that the Academy will monitor my use of the ICT systems, email and other digital communications
- I understand that the rules set out in this agreement also apply to use of the Academy ICT systems (e.g. laptops, email, VLE etc) out of the Academy, and to the transfer of personal data (digital or paper based) out of the Academy
- I understand that the Academy ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person
- I will not communicate with students through social networking sites such as Facebook or on Twitter. I will not under any circumstances accept friend requests from a person who I believe to be either a parent/carer or a student at the Academy. I am responsible for ensuring that privacy settings are enabled, and that private content is not available to students. If I require support with this the IT staff will help me
- I will not issue my mobile phone number to students or ask for students' mobile phone numbers or keep a record of student mobile phone numbers for reasons other than official Academy business e.g. speaking to parents
- I will not use personal devices (including Smartphones, tablets or other recording equipment) to capture audio, video or images of others

I will be professional in my communications and actions when using Academy ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language, and I appreciate that others may have different opinions
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the Academy's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so.

- I will not use chat and social networking sites in the Academy in accordance with the Academy Policy
- I will only communicate with students and parents/carers using official Academy systems. Any such communication will be professional in tone and manner, and any protracted communication will be referred to my line manager
- I will not engage in any on-line activity that may compromise my professional responsibilities

The Academy has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the Academy:

- When I use my mobile devices (PDAs/laptops/mobile phones/USB devices etc) in the Academy, I will follow the rules set out in this agreement, in the same way as if I was using Academy equipment. I will also follow any additional rules set by the Academy about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses
- I will not use personal email addresses on the Academy ICT systems
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs)
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programs or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work
- I will not install or attempt to install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings, unless this is allowed in Academy policies
- I will not disable or cause any damage to Academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Academy Personal Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Academy policy to disclose such information to an appropriate authority
- I will immediately report any damage or faults involving equipment or software; however, this may have happened

When using the internet in my professional capacity or for Academy sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos)

I understand that I am responsible for my actions in and out of the Academy:

- I understand that this Acceptable Use Policy applies not only to my work and use of Academy ICT equipment in the Academy, but also applies to my use of Academy ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the Academy
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the Academy's ICT systems (both in and out of the Academy) and my own devices (in the Academy and when carrying out communications related to the Academy) within these guidelines.

Student - Acceptable Use Policy Agreement

I understand that I must use Academy ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the Academy will monitor my use of the systems, devices and digital communications
- 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. I understand that I should not write down or store a password where it is possible that someone may steal it
- I will be aware of "stranger danger", when I am communicating on-line
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online
- I will not use personal devices (including Smartphones, tablets or other recording equipment) to capture audio, video or images of others

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the Academy systems and devices are intended for educational use and that I will not use them for personal or recreational use
- I will not try to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work
- I will not use the Academy systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube)

I will act as I expect others to act toward me:

- 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
- 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
- I will not take or distribute images of anyone without their permission

I recognise that the Academy has a responsibility to maintain the security and integrity of the technology it offers me and to ensure its smooth running:

- I will only use my own personal devices (mobile phones/USB devices etc) in the Academy if I have permission. I understand that, if I do use my own devices in the Academy, I will follow the rules set out in this agreement, in the same way as if I was using Academy equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will immediately report any damage or faults involving equipment or software; however, this may have happened
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programs of any type on any Academy device, nor will I try to alter computer settings
- I will not use social media sites

When using the internet, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me

Use of Artificial Intelligence:

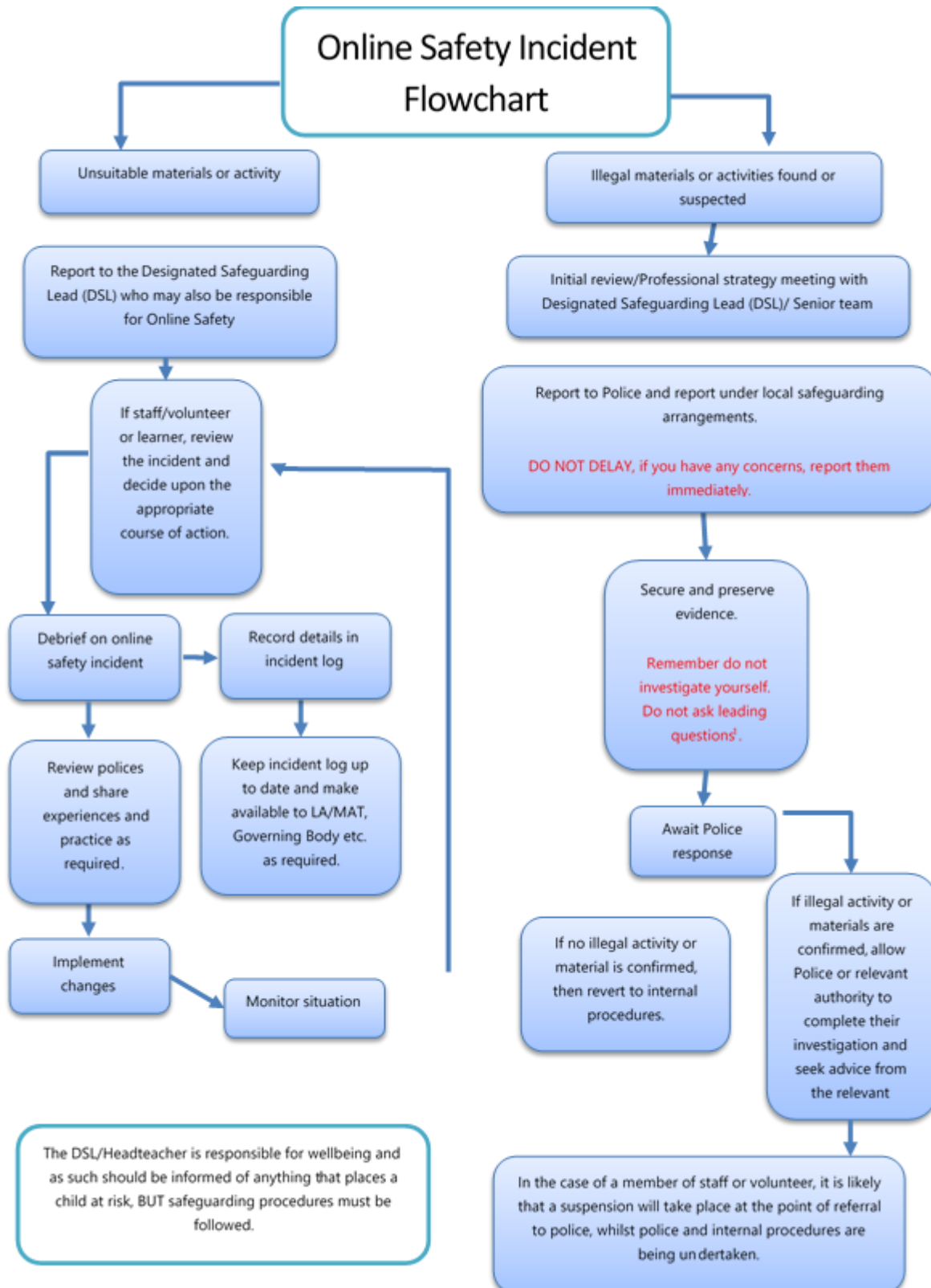
- I understand that I must reference the use of Artificial Intelligence in any assessments I undertake.
- I understand that passing work generated by Artificial Intelligence as my own and without reference is classed as plagiarism.

I understand that I am responsible for my actions, both in and out of the Academy:

- I understand that the Academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, which are covered in this agreement, when I am out of Academy and where they involve my membership of the Academy community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the Academy network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

In the event of suspicion, all steps in this procedure should be followed:

Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.

Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse)

Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:

- Internal response or discipline procedures
- Involvement by Local Authority or national/local organisation (as relevant)
- Police involvement and/or action

If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation

It is important that all the above steps are taken as they will provide an evidence trail for the Academy and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Academy Actions & Sanctions

Students

Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities)	X		X	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X				X	X	X	X	X
Unauthorised use of mobile phone/digital camera another mobile device	X	X							X
Unauthorised use of social media/ messaging apps/personal email	X	X			X		X	X	X
Unauthorised downloading or uploading of files	X	X			X		X	X	X
Allowing others to access Academy network by sharing username and passwords					X		X	X	X
Attempting to access or accessing the Academy network, using another student's account					X			X	X

Online Safety POLICY

Attempting to access or accessing the Academy network, using the account of a member of staff	X	X			X	X		X	X
Corrupting or destroying the data of other users	X	X			X		X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X			X		X		X
Actions which could bring the Academy into disrepute or breach the integrity of the ethos of the Academy					X	X	X	X	X
Using proxy sites or other means to subvert the Academy's filtering system	X	X			X		X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident								X	
Deliberately accessing or trying to access offensive or pornographic material	X	X			X		X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act								X	

Staff**Actions / Sanctions**

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities)		X	X	X	X	X	X	X
Inappropriate personal use of the internet/social media personal email	X				X	X		
Unauthorised downloading or uploading of files	X				X	X		
Allowing others to access the Academy's network by sharing username and passwords or attempting to access or accessing the Academy's network, using another person's account					X	X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X				X	X		
Deliberate actions to breach data protection or network security rules	X				X	X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X			X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X		X	X	X	X	X

Online Safety POLICY

Using personal email/social networking/instant messaging/text messaging to carry out digital communications with students	X				X	X		
Actions which could compromise the staff member's professional standing	X				X	X		
Actions which could bring the Academy into disrepute or breach the integrity of the ethos of the Academy	X	X			X	X		
Using proxy sites or other means to subvert the Academy's filtering system	X				X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X				X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X		X	X	X		X
Breaching copyright or licensing regulations	X				X	X		
Continued infringements of the above, following previous warnings or sanctions	X	X			X	X	X	X

Online Safety Education Programme

While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the Academy's online safety provision. Learners need the help and support of the Academy to recognise and avoid online safety risks and develop their resilience.

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for:

"a carefully sequenced RSHE curriculum, based on the Department for Education's (DfE's) statutory guidance, that specifically includes sexual harassment and sexual violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of 'nudes'."

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways

A planned online safety curriculum for all year groups matched against a nationally agreed framework e.g. Education for a Connected Work Framework by UKCIS/DCMS and regularly taught in a variety of contexts.

- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- Incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- The programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside the Academy
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit

Online Safety POLICY

- It is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- The online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

Staff/Volunteers

The DfE guidance “Keeping Children Safe in Education” states:

“All staff should receive appropriate safeguarding and child protection training (including online safety) at induction. The training should be regularly updated. In addition, all staff should receive safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively.”

“Governing bodies and proprietors should ensure... that safeguarding training for staff, including online safety training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning.”

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- Training will be an integral part of the Academy’s annual safeguarding and data protection training for all staff
- New staff will receive online safety training as part of their induction programme, ensuring that they fully understand the Academy online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours
- Online Safety Lead and Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / MAT / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations
- The Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- The Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

Contribution of Learners

The Academy acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the Academy community and how this contributes positively to the personal development of young people. Student contribution is recognised through:

- Mechanisms to canvass learner feedback and opinion.
- Learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns
- learners designing/updating acceptable use agreements
- Contributing to online safety events with the wider Academy community e.g. parents' evenings, family learning programmes etc.

Smoothwall Cloud Filter

Full Cloud Device Overview

For all cloud-compatible devices, the Smoothwall cloud filter client can be pushed out to users on Windows, Chromebooks, MacOS, IOS & Android. Devices that have the client then connect to the Smoothwall cloud platform to pull down a copy of the policies. From there the client device starts filtering the user's internet traffic locally and stores the data captured locally. This enables this element to be incredibly flexible, as the client does all the hard work, meaning it is highly scalable. Another benefit to the cloud extension filter is that it can inspect SSL content without breaking the encryption with a man-in-the-middle certificate, meaning less administrative overhead. Authentication is also simplified as the user ID is taken from the currently logged-on user, without having to verify credentials against a traditional directory such as AD.

Smoothwall cloud filtering is deployed differently depending on the type of device it is being installed on.

Windows

The smoothwall cloud client can be rolled out to the following windows operating systems, Windows 10, Windows 11 & Windows 11 SE. The client is to be rolled out via the management platform in place (Typically InTune or GPO). Full dynamic content filtering will be compatible on either edge or chrome browsers. Whilst anything off the browser such as applications will be filtered via a DNS backstop filter.

Chrome

A smoothwall cloud extension is pushed out to chromeOS devices. Smoothwall supports minimum chrome 110 for MV3 deployment. However, smoothwall can accommodate for anything earlier by deployment of the MV2 extension. The extension is typically pushed out via google admin suite. As the whole device is running on chrome, smoothwall cloud filter works well with Chromebook and can dynamically filter all content.

IPAD

iPad Cloud Filter is achieved by leveraging a customer Smoothwall browser which is deployed via your MDM of choice. Alongside the custom Smoothwall browser configuration settings are applied which will use your MDM's configuration to identify the user based on the designated username in a 1:1 iPad deployment. By doing this your iPad users can be filtered and reported on accurately whilst using the Smoothwall browser.

It is important to note that if an iPad is physically shared around between a class, then we cannot achieve full user-based filtering/reporting however we can implement semi-granular filtering by using your MDM to apply certain usernames to iPads in use so that we can target specific iPads or groups of iPads with web filtering to ensure all iPads are filtered appropriately.

MacOS

Smoothwall Cloud Filter for macOS provides robust and reliable web filtering exclusively within the Chrome browser on Apple devices, whether they are on or off the school network. To ensure consistent and effective safeguarding, all other browsers must be removed from the devices, as filtering will only be applied within the managed Chrome environment through a lightweight client and browser extension. This focused approach guarantees the enforcement of your safeguarding policies, blocking inappropriate content and providing detailed reporting on user activity solely within the Chrome browser.

Android

The Android Filter app is compatible with a broad range of managed Android devices including tablets and smartphones, with these requirements:

Devices must be running Android 11.0 (Red Velvet Cake) or higher.

Devices must be managed through a Mobile Device Management (MDM) solution for deployment and management. The Android filter app can be deployed via google admin or Intune.

Cloud Only Deployment Overview

Smoothwall filter can easily be deployed as a cloud only solution, without the need of a physical appliance. This deployment is the quickest type and the most cost effective. The cloud filter client can be deployed on the Windows, Chromebooks, Android, Mac and iOS whilst utilising directories such as AzureAD/Entra, Google Directory and AD to support user ID/authentication. With this model utilising the Smoothwall cloud filter it provides offsite and onsite filtering, so users are protected whilst browsing the internet wherever they are.

Smoothwall cloud filters will only be applied to managed devices which are controlled by the organisation. Anything which is unmanaged will utilise DNS based filtering.

This leads to managed devices being fully dynamically content filtered with identification whilst non managed devices are DNS filtered with no identification. This is all dependent on the schools/organisation's requirement. If the site required dynamic content filtering for non-managed devices, an appliance will be recommended leading back to a hybrid deployment instead.

Smoothwall Monitor

Monitor Overview

Smoothwall Monitor is a proactive and comprehensive digital safeguarding solution designed to provide educational institutions with enhanced visibility of online and offline activities, ensuring a safer learning environment for students. At its core, Smoothwall Monitor offers real-time digital keystroke monitoring, capturing and analysing text input across a wide range of applications and platforms.

The system goes beyond automated analysis by incorporating a 24/7/365 alerting service with a UK based human moderation team. This crucial element ensures that critical alerts are promptly reviewed and validated by trained safeguarding professionals, minimising false positives and prioritising genuine risks. This approach enables schools to respond effectively to potential threats, intervene proactively, and provide timely support to students in need.

Smoothwall Monitor's features include:

- **Keystroke Capture and Analysis:** Detailed recording of text input across applications, browsers, and platforms.
- **24/7/365 Alerting Service:** Continuous monitoring and alert triage by trained safeguarding professionals to ensure timely intervention.
- **Customizable Policies and Thresholds:** Adaptable settings to align with specific school policies and risk thresholds.
- **Reporting and Analytics:** Comprehensive reporting tools to track trends, analyse incidents, and demonstrate compliance.
- **Integration with Existing Systems:** Seamless integration with other safeguarding platforms and school management systems.

By providing a robust and proactive monitoring solution, Smoothwall Monitor empowers educational institutions to create a safer digital environment, protect students from online harm, and fulfil their safeguarding responsibilities effectively.

Cloud Only Monitor Deployment Overview

A Cloud Only Monitor deployment involves installing the Smoothwall Monitor client on end-user devices and managing groups and directories without needing an on-premises Smoothwall appliance. This streamlined approach leverages Smoothwall's cloud infrastructure for monitoring and alert management.

Smoothwall Moderation Team

Smoothwall's commitment to comprehensive online safeguarding is exemplified by its dedicated Moderation Team, a vital component of its proactive approach to protecting children in the digital space. Operating 24 hours a day, 7 days a week, 365 days a year, this team provides a crucial layer of human expertise and intervention, complementing the advanced AI technology that forms the foundation of Smoothwall's safeguarding solutions.

This is where the Moderation Team's expertise becomes indispensable. Composed of highly trained safeguarding professionals, these moderators bring a wealth of knowledge and experience in child development, online behaviour, and best practices in safeguarding. They meticulously review and validate alerts generated by the technology, providing a crucial human element that reduces false positives, ensures accurate assessment of risk, and prioritises the most critical cases. The Smoothwall Moderation Team acts as a critical bridge between technology and human intervention, providing a robust and reliable safeguarding service that empowers educational institutions to protect children effectively in the online world.

Monitor Windows

Smoothwall Monitor on Windows operates at the operating system level, enabling comprehensive keystroke monitoring across any text field, regardless of the application. This deep integration allows for the capture and analysis of text input within any programme, ensuring no activity goes unseen. By installing at the OS level, Smoothwall Monitor gains the necessary access to monitor all keystrokes, providing a holistic view of user activity for safeguarding purposes. This method ensures that even text entered into less common applications or custom software is captured and analysed, offering a robust and thorough monitoring solution. For Windows systems, Smoothwall Monitor is provided as an MSI package, facilitating streamlined installation and deployment.

Monitor Chromebooks

Smoothwall Monitor on Chromebooks is deployed as a browser extension. This extension is specifically attached to the user's Google account. This means that when a user logs into any managed Chromebook with their account, the Smoothwall Monitor extension automatically activates and begins monitoring their activity. This user-centric approach ensures that monitoring follows the individual across all Chromebooks they use, providing consistent oversight regardless of which Chromebook they are logged into.

Monitor iPads

Smoothwall Monitor's safeguarding capabilities on iPads are intrinsically linked to the Smoothwall Cloud Filter and rely on the use of the Smoothwall Browser. This specialised browser is a crucial component of the Smoothwall ecosystem on iOS, enabling the necessary level of monitoring and control required for effective online safeguarding. Due to Apple's stringent security protocols on iPads, which significantly restrict the capabilities of third-party applications, Smoothwall's monitoring functionality can only operate within the confines of the Smoothwall Browser. This means that to ensure comprehensive and effective monitoring of student activity on iPads, it becomes essential to replace any other browsers currently deployed on these devices, such as Safari or Chrome with the Smoothwall Browser.

Online Safety POLICY

The limitations imposed by Apple's security measures prevent Smoothwall from directly monitoring activity within other browsers. Consequently, if students can use alternative browsers, their online actions may not be fully captured and analysed by Smoothwall Monitor, potentially creating blind spots in safeguarding efforts. The Smoothwall Browser, therefore, becomes the gateway for both filtered internet access and effective monitoring, ensuring that all online activity is subject to the necessary scrutiny. This approach allows Smoothwall to maintain a controlled and secure environment, enabling proactive identification and intervention in potential safeguarding incidents.

The need for browser replacement is a direct consequence of Apple's security architecture, which prioritises user privacy and system integrity, but this necessitates a shift in browser deployment strategy to facilitate robust online safeguarding.