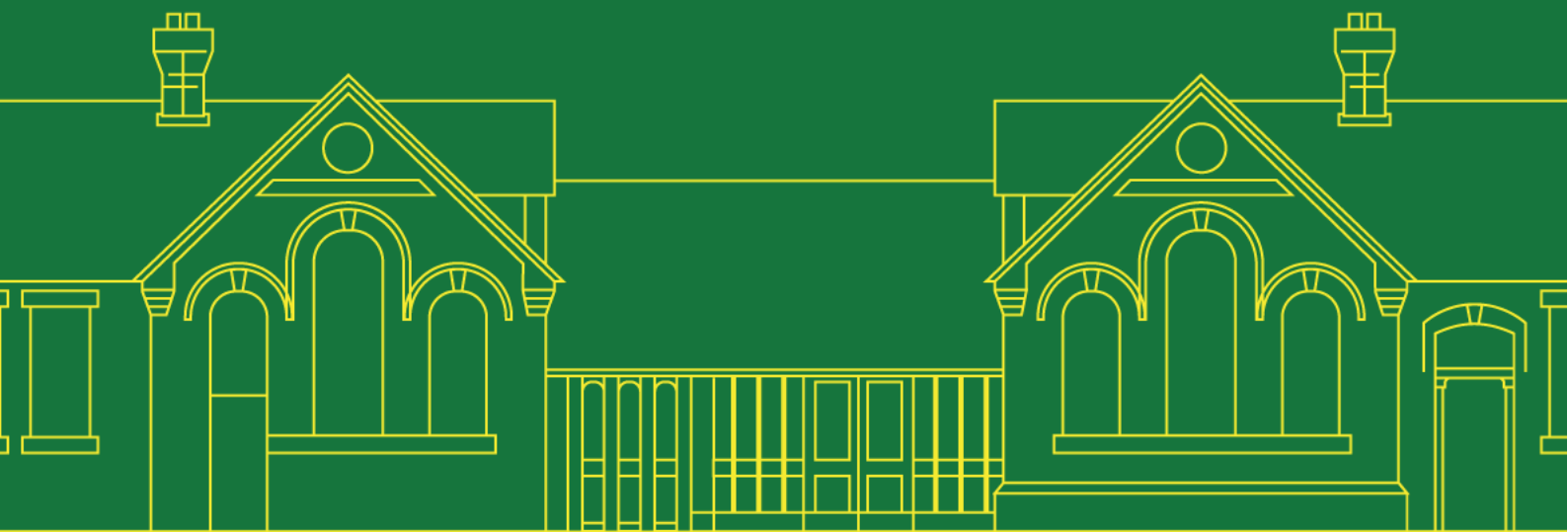




Online Safety Policy

September 2026 (Review September
2027)



**STOUR VALE
ACADEMY
TRUST**

ONLINE SAFETY POLICY – SEPTEMBER 2026

Approved at

LGB Meeting – 14th October 2026

Signed by Chair of Governors:

A handwritten signature in black ink, appearing to read 'P Ramage', with a stylized flourish at the end.

Mr P Ramage

Date signed:

14th October 2026

Review of Policy

September 2027

Queen Victoria Primary School Vision and Values

At Queen Victoria Primary School, we care deeply for the children of Sedgley; we believe every child is worthy and capable of success and happiness and this shows in every interaction. We create the conditions for children to grow into individuals who care about themselves, each other and the world they live in. We strive to make a positive difference by basing everything we do on our CARE principles:

Children are at the heart of everything we do – every day, in every decision, and every action, children's best interests and needs are put first. We have a team of compassionate staff who will move heaven and earth to ensure children get what they need to succeed.

Aspiration – We are full of hope, ambition, and the highest expectations for all children to have bright futures. Therefore, we are ambitious in the curriculum we offer and the standards we expect of ourselves.

Responsible – One of our key purposes is to help our children develop into respectful and responsible citizens who make positive contributions to life in Sedgley and beyond.

Excellence – We are relentless in our pursuit of providing excellence in education, with a balanced approach to academic achievement and personal development.

Aims and Principles

At Queen Victoria Primary School, we recognise that technology plays an important role in children's education, communication and everyday lives. We are committed to ensuring that all pupils develop the knowledge, skills and confidence to use technology safely, responsibly and respectfully.

Our approach to online safety reflects our CARE values and aims to:

- Protect pupils, staff and the wider school community from online harm.
- Equip pupils with the knowledge and skills to recognise risks, make informed decisions and seek help when needed.
- Promote positive, respectful and responsible behaviour online.
- Ensure that appropriate safeguarding, filtering and monitoring arrangements are in place.
- Provide additional support and appropriately adapted education for pupils who may be particularly vulnerable to online harm.
- Work in partnership with parents and carers to promote online safety both in school and at home.
- Ensure that online safety is embedded throughout the curriculum and wider safeguarding culture of the school.

Our approach recognises four broad categories of online risk:

- **Content:** Exposure to harmful, inappropriate or illegal material, including violent or sexual content, extremism, misinformation and content promoting harmful behaviours.
- **Contact:** Harmful interactions with others online, including bullying, grooming, exploitation and inappropriate contact through social media, gaming platforms or artificial intelligence applications.
- **Conduct:** Behaviour that creates risks for individuals or others, including cyberbullying, sharing personal information or images, and inappropriate online communication.
- **Commerce:** Risks associated with online advertising, scams, phishing, financial exploitation and gambling.

All staff must understand the four categories of online risk, recognise when a child may be experiencing harm and report concerns to the DSL. These risks include self-harm and suicide content, misogyny and hate speech, misinformation and conspiracy theories, AI-generated sexual imagery, coercion and financial scams.

Scope of the Online Safety Policy

This policy applies to all members of the Queen Victoria Primary School community, including pupils, staff, governors, volunteers, parents/carers, visitors and other individuals who access or use the school's digital technology systems.

The policy covers the safe, responsible and appropriate use of digital technology, including school-owned and personal devices, internet access, online platforms, communication systems, social media and artificial intelligence (AI).

It applies to the use of technology both within school and, where relevant, outside school when online activity has an impact on the safety, wellbeing or education of members of the school community.

The school recognises that online safety is an integral part of safeguarding and that risks can arise both within and beyond the school environment. We are committed to educating and protecting pupils, promoting responsible digital citizenship and responding appropriately to online safety concerns.

Where online incidents occur outside school but affect pupils or the wider school community, the school will respond in accordance with its safeguarding responsibilities and relevant policies, including the Behaviour Policy and Anti-Bullying Policy. Parents and carers will be involved where appropriate, taking account of safeguarding considerations.

Policy Communication and Review

The policy will be reviewed annually and updated during the year where incidents, local safeguarding trends or changes in technology require this. Staff, governors, pupils and parents/carers will contribute to review where appropriate. Changes will be communicated

promptly through induction, safeguarding updates, the school website and the relevant acceptable use agreements.

Legislation and Guidance

This policy has been developed with reference to relevant legislation, statutory guidance and national recommendations relating to safeguarding, education, online safety and the responsible use of technology.

In particular, it takes account of:

- Keeping Children Safe in Education (DfE) – statutory guidance setting out schools' safeguarding responsibilities, including online safety, child-on-child abuse, filtering and monitoring, and the management of online safeguarding concerns.
- Filtering and Monitoring Standards for Schools and Colleges (DfE) – establishing expectations for appropriate filtering and monitoring systems, clearly defined responsibilities and regular review of their effectiveness.
- Teaching Online Safety in Schools (DfE) – guidance supporting schools to provide effective online safety education throughout the curriculum.
- Relationships Education, Relationships and Sex Education (RSE) and Health Education (DfE) – statutory guidance, including the expectations for teaching pupils about online relationships, respectful behaviour, privacy and managing online risks.
- National Curriculum in England: Computing Programmes of Study (DfE) – setting out expectations for pupils to use technology safely, respectfully, responsibly and securely.
- Searching, Screening and Confiscation: Advice for Schools (DfE) – guidance on the lawful searching and confiscation of electronic devices and the management of inappropriate or harmful content.
- Mobile Phones in Schools (DfE) – guidance on restricting pupils' access to mobile phones and similar smart technology during the school day.
- Prevent Duty Guidance – setting out responsibilities for protecting children from the risks of radicalisation and extremism, including online.

As a member of Stour Vale Academy Trust, Queen Victoria Primary School operates in accordance with relevant trust-wide policies and procedures, including the *Safeguarding and Child Protection Policy*, *Data Protection Policy*, and *Cyber Security Policy*. This policy should be read alongside these trust policies and the school's relevant safeguarding, behaviour, anti-bullying and curriculum policies.

Roles and Responsibilities

Online safety is a shared responsibility across the school community. All staff have a duty to promote safe and responsible use of technology, recognise potential online risks and report concerns promptly. Specific responsibilities are outlined below.

The Local Governing Body

The Local Governing Body is responsible for monitoring the implementation of this policy and holding the headteacher to account for its effectiveness, within the governance arrangements of Stour Vale Academy Trust.

The Local Governing Body will:

- Ensure that online safety is embedded within the school's approach to safeguarding and is considered alongside other relevant policies and procedures.
- Ensure that appropriate arrangements are in place for filtering and monitoring, including an annual review of their effectiveness.
- Receive information about online safety incidents, emerging risks and the effectiveness of the school's safeguarding arrangements through reports from the headteacher and Designated Safeguarding Lead (DSL).
- Ensure that staff receive appropriate online safety training and regular updates, including their responsibilities in relation to filtering and monitoring.
- Monitor the effectiveness of online safety education, ensuring that pupils develop the knowledge and skills needed to keep themselves safe online.
- Ensure that online safety education and safeguarding arrangements are appropriately adapted to meet the needs of vulnerable pupils and those with special educational needs and/or disabilities (SEND).

All governors are expected to understand this policy and adhere to the school's acceptable use requirements.

Headteacher and Senior Leaders

The headteacher has overall responsibility for ensuring that this policy is implemented consistently and that online safety is embedded within the school's safeguarding culture.

The headteacher, supported by senior leaders, will:

- Ensure that all staff understand their online safety responsibilities and receive appropriate training.
- Ensure that clear procedures are in place for reporting, recording and responding to online safety concerns.
- Work with the DSL and technical support provider to ensure that appropriate filtering, monitoring and technical security arrangements are in place.
- Ensure that responsibilities for managing and reviewing filtering and monitoring systems are clearly defined.
- Ensure that the school's use of digital technologies, online platforms and artificial intelligence is appropriately risk-assessed and complies with relevant safeguarding, data protection and trust requirements.
- Support the DSL in responding to significant online safety incidents and liaising with external agencies where necessary.

- Ensure that the Local Governing Body receives appropriate information about online safety arrangements, incidents and emerging risks.

The Designated Safeguarding Lead (DSL)

The DSL takes lead responsibility for online safety as part of the school's wider safeguarding arrangements. Details of the DSL and deputy DSLs are set out in the school's Child Protection and Safeguarding Policy.

The DSL will:

- Maintain an up-to-date understanding of online safeguarding risks, including those associated with harmful content, online contact, cyberbullying, child-on-child abuse, exploitation and artificial intelligence.
- Act as the main point of contact for online safety safeguarding concerns, ensuring that incidents are appropriately recorded on CPOMS and responded to in accordance with safeguarding procedures.
- Work with the headteacher, senior leaders and technical support provider to understand the filtering and monitoring systems in place and ensure that concerns identified through these systems are reviewed and acted upon.
- Contribute to the annual review of filtering and monitoring arrangements, ensuring that these reflect the school's safeguarding needs and the risks faced by pupils.
- Work with the computing lead and other curriculum leaders to ensure that online safety education responds to emerging risks and the needs of pupils.
- Ensure that staff receive appropriate safeguarding updates relating to online safety, including how to recognise, respond to and report concerns.
- Liaise with parents/carers, external agencies and safeguarding partners where appropriate.
- Provide regular information to the headteacher and Local Governing Body about online safety incidents, trends and areas for development.
- Contribute to the review and updating of this policy.

In the absence of the DSL, deputy DSLs will carry out these responsibilities in accordance with the school's safeguarding arrangements.

The Managed Service Provider

The school's managed IT service provider, Agilisys, provides technical support for the school's IT infrastructure, security systems and filtering and monitoring arrangements, working alongside the headteacher, School Business Manager and DSL.

Within the scope of its agreed service responsibilities, the provider will:

- Implement and maintain appropriate technical security measures to protect school systems, devices and networks.

- Support the operation and maintenance of filtering and monitoring systems to reduce pupils' exposure to harmful and inappropriate online content.
- Undertake appropriate system maintenance, security updates and technical checks.
- Support the school in identifying and responding to technical security concerns, including potential cyber incidents and data breaches.
- Provide technical information and advice to support the school's regular and annual reviews of filtering and monitoring arrangements.
- Escalate relevant technical and safeguarding concerns to the appropriate school or trust personnel in accordance with agreed procedures.

The school retains responsibility for ensuring that technical arrangements meet its safeguarding needs. Safeguarding decisions arising from monitoring alerts or online incidents remain the responsibility of the school's safeguarding team.

Agilisys and LGfL will work with the DSL and Matthew Priest to document their respective technical responsibilities, reporting arrangements and escalation routes. Lynne Perkins will support coordination with the providers and Stour Vale Academy Trust. New devices and services must have appropriate filtering and monitoring in place before release to users.

The Computing Lead and Curriculum Leaders

The computing lead, working alongside the DSL and other curriculum leaders, is responsible for supporting the planning, delivery and development of online safety education across the school.

Responsibilities include:

- Ensuring that online safety is taught progressively through the computing curriculum, including the use of Purple Mash 2BeSafe.
- Working with PSHE leaders to ensure that online safety is reinforced through relationships and health education.
- Supporting teachers to deliver age-appropriate online safety lessons that develop pupils' understanding of risks and strategies for keeping themselves safe.
- Ensuring that online safety education addresses relevant and emerging issues, including digital wellbeing, cyberbullying, misinformation, privacy and the responsible use of AI.
- Supporting the adaptation of online safety teaching to meet the needs of pupils with SEND and other vulnerabilities.
- Promoting online safety through assemblies, national initiatives such as Safer Internet Day and wider curriculum opportunities.
- Reviewing the effectiveness of online safety education and identifying opportunities for further development.

The PSHE and relationships education lead will work with the computing lead and DSL to ensure complementary, age-appropriate teaching about consent, healthy relationships, mental

wellbeing, online risks and respectful behaviour. Subject leaders will identify opportunities to reinforce these messages across their subjects and consider online safety in relevant action plans.

The Data Protection Officer will advise on privacy, information security, appropriate access to records and the assessment of new technologies. Data protection requirements must support lawful information sharing to safeguard children; they must not be used as a reason to withhold necessary safeguarding information.

All Teaching Staff, Support Staff and Volunteers

All staff, including teaching staff, support staff, temporary staff and volunteers, have a responsibility to promote online safety and model appropriate use of technology.

They are expected to:

- Read, understand and follow this policy, the school's safeguarding procedures and relevant acceptable use agreements.
- Maintain appropriate professional conduct when using technology, including social media, messaging services and online communication platforms.
- Use school-approved systems for professional communication and the storage or processing of school information.
- Follow the school's requirements for the safe and responsible use of AI, including protecting personal and confidential information.
- Supervise pupils' use of technology appropriately and reinforce online safety expectations.
- Remain vigilant to online safeguarding risks and report concerns promptly to the DSL, recording them on CPOMS where appropriate.
- Respond appropriately to disclosures or concerns involving harmful online content, cyberbullying, online exploitation or inappropriate image sharing.
- Participate in relevant online safety training and updates.
- Report concerns about the security, filtering or monitoring of school systems through the appropriate channels.

Pupils

Pupils are expected to use technology safely, respectfully and responsibly, in accordance with their age and understanding.

They will be supported to:

- Follow the school's acceptable use agreements and expectations for online behaviour.
- Treat others with kindness and respect when communicating or interacting online.
- Protect their personal information and respect the privacy of others.
- Recognise potentially harmful or inappropriate online content, contact and behaviour.

- Tell a trusted adult if they encounter something online that makes them feel uncomfortable, worried or unsafe.
- Understand that online actions can have consequences for themselves and others.
- Develop the knowledge and skills needed to make safe, informed choices when using digital technology.

Parents and Carers

Parents and carers play an important role in supporting children to develop safe and responsible online habits.

The school encourages parents and carers to:

- Reinforce the online safety messages taught in school.
- Support their children to use devices, games, apps and online platforms in an age-appropriate and responsible way.
- Maintain an open dialogue with their children about their online experiences.
- Report concerns about online behaviour or incidents affecting their child's safety or wellbeing to the school.
- Support the school's acceptable use expectations and relevant policies.

The school will provide information and guidance to help parents and carers understand online risks and support their children's digital wellbeing.

Visitors and Members of the Community

Visitors, contractors and other individuals using the school's digital systems or internet connection are expected to follow relevant online safety and acceptable use requirements. Any online safety or safeguarding concerns identified by visitors must be reported promptly to a member of the school's safeguarding team.

Volunteers, Contractors and External Groups

Volunteers, contractors, tutors and external groups using school technology must follow the relevant acceptable use requirements, report concerns to the DSL and model safe, professional conduct. Contractors and tutors must not arrange private meetings or communicate directly with pupils without the school's prior knowledge and approval. External groups and parent associations must protect others' images and information and behave respectfully online.

Online Safety Education

At Queen Victoria Primary School, we recognise that developing the knowledge, skills and understanding to stay safe online is an essential part of preparing children for life in an increasingly digital world. We are committed to providing a progressive, age-appropriate

approach to online safety education that enables pupils to use technology safely, respectfully, responsibly and confidently.

Online safety education is embedded within our computing curriculum and reinforced through Personal, Social, Health and Economic (PSHE) education, relationships and health education, assemblies and wider curriculum opportunities. Our approach reflects the school's CARE values, particularly our commitment to helping children become responsible, respectful citizens who care for themselves and others.

Online Safety Within the Curriculum

Online safety is taught explicitly through our computing curriculum, which incorporates Purple Mash 2BeSafe resources to support the systematic development of pupils' knowledge and understanding. Learning is revisited and built upon as children progress through school, reflecting their increasing independence and the changing digital environments they encounter.

Teaching is informed by the National Curriculum for Computing and the statutory requirements for relationships and health education.

In Key Stage 1, pupils are taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

In Key Stage 2, pupils are taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about online content and contact.
- Be discerning when evaluating digital content.

Alongside these expectations, the school's online safety curriculum develops pupils' understanding of:

- **Online relationships and behaviour:** treating others with respect, recognising inappropriate behaviour, understanding online bullying and knowing how to seek help.
- **Privacy and personal information:** protecting personal information, understanding privacy settings and recognising the potential consequences of sharing information, images and videos.
- **Online contact:** recognising that people may not always be who they claim to be, understanding the risks of communicating with strangers and knowing how to respond to unwanted or concerning contact.
- **Online content and critical thinking:** recognising unreliable information, misinformation, harmful content and the importance of questioning what they see and read online.

- **Digital footprints and reputation:** understanding that information shared online can be copied, circulated and difficult to remove.
- **Digital wellbeing:** developing healthy habits around screen time, online interactions and the balance between digital activities and other aspects of life.
- **Online security:** developing age-appropriate understanding of passwords, account security, scams and how to protect themselves and their information.
- **Artificial intelligence:** developing an age-appropriate awareness that online images, videos and information may be generated or manipulated using AI, and the importance of using these technologies safely, critically and responsibly.

By the end of primary school, pupils will have been taught the knowledge and strategies needed to recognise and respond to common online risks, understand the importance of respectful online relationships, protect their personal information and know how and where to seek help.

Teaching Approaches

Online safety education is delivered through planned lessons, discussion, practical activities and opportunities to explore realistic scenarios. Teaching encourages pupils to think critically, make informed decisions and develop the confidence to respond appropriately when they encounter online risks.

Online safety messages are reinforced across the curriculum whenever pupils use digital technology or access online resources. Staff model safe and responsible technology use and take opportunities to reinforce appropriate online behaviour.

The school also promotes online safety through assemblies, awareness campaigns and national initiatives, including Safer Internet Day and Anti-Bullying Week.

Supporting All Pupils

We recognise that children's experiences of technology, levels of understanding and vulnerability to online harm vary considerably.

Online safety teaching is adapted where necessary to meet the needs of individual pupils, including those with special educational needs and/or disabilities (SEND), pupils with additional safeguarding vulnerabilities and those who may require further support to recognise and respond to online risks.

Teachers use appropriate language, resources, repetition and practical examples to ensure that online safety messages are accessible and meaningful. Where specific risks or concerns are identified, additional teaching or targeted support may be provided in consultation with the Designated Safeguarding Lead (DSL) and other relevant staff.

Responding to Emerging Risks

Online safety education is reviewed regularly to ensure that it remains relevant to pupils' experiences and reflects developments in technology, online platforms and emerging risks. The computing lead, working alongside the DSL and PSHE lead, will consider information from safeguarding concerns, pupil voice, staff observations and national guidance to identify any additional learning needs.

Where particular online safety concerns arise, the school may provide additional teaching, assemblies or targeted interventions to reinforce key messages and support pupils in making safe and responsible choices.

Above all, we aim to create a culture in which children feel confident to talk to trusted adults about their online experiences, understand that they will be listened to and know that support is available whenever they encounter something that worries or upsets them.

Staff will consider the age appropriateness and risks of online tasks, including homework, and support pupils with safe searching, critical thinking, copyright and seeking help. Safeguarding records, filtering and monitoring reports, pupil voice, parental concerns and staff feedback will inform curriculum priorities. Pupils will be supported without fear-based or victim-blaming language.

Supporting Parents with Online Safety

The school will provide information to parents and raise awareness of internet safety through:

- Newsletter, letters to families or other communications home
- our website and social media.
- Parent workshops
- Campaigns or events (such as Safer Internet Day)
- Parents' evenings and information/induction evenings
- Curriculum activities
- Signposting relevant information

We will inform parents about:

- The systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

This policy will also be shared with parents via the school website.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Online Safety Training for Staff and Governors

Queen Victoria Primary School recognises that effective online safety depends on all staff and governors having the knowledge and understanding needed to identify risks, promote safe and responsible use of technology and respond appropriately to concerns.

Online safety training forms an integral part of the school's wider safeguarding training programme and is reviewed regularly to reflect emerging risks, changes in technology and updates to statutory guidance.

Staff Training

All staff, including teaching staff, support staff and other adults working in school, will receive appropriate online safety training as part of their induction and ongoing safeguarding professional development.

Training will be refreshed at least annually, with additional updates provided throughout the year as necessary through staff briefings, safeguarding updates and other professional development opportunities.

Training will ensure that staff:

- Understand their responsibilities for safeguarding pupils online and the procedures for identifying, reporting and recording online safety concerns.
- Recognise the range of online risks that children may encounter, including harmful content, inappropriate contact, cyberbullying, online exploitation, grooming, radicalisation and child-on-child abuse.
- Understand how technology may be used to facilitate sexual harassment, coercion and the sharing of inappropriate or intimate images, including AI-generated or manipulated content.
- Understand the school's filtering and monitoring arrangements, their individual responsibilities and how to report concerns about inappropriate content, monitoring alerts or failures in filtering systems.
- Recognise that filtering and monitoring systems do not remove the need for appropriate supervision and professional vigilance.
- Understand the school's expectations for professional conduct online, including the appropriate use of social media, communication platforms, personal devices and school technology.
- Understand the risks and responsibilities associated with the use of artificial intelligence, including data protection, confidentiality, safeguarding and the need to use approved systems appropriately.

- Know how to support pupils in developing safe, respectful and responsible online behaviours, including reinforcing online safety messages across the curriculum.
- Recognise that some pupils, including those with special educational needs and/or disabilities (SEND) or additional safeguarding vulnerabilities, may require adapted approaches to online safety education and support.

All staff are expected to maintain an awareness of emerging online safety issues and follow the school's safeguarding procedures when concerns arise.

Designated Safeguarding Lead and Senior Leaders

The Designated Safeguarding Lead (DSL) and deputy DSLs will receive appropriate training and updates to maintain their knowledge of online safeguarding risks and effective responses to online incidents.

The headteacher, DSL and relevant senior leaders will ensure that they understand the school's filtering and monitoring arrangements, including the roles and responsibilities of those involved in managing, reviewing and responding to concerns identified through these systems.

Relevant leaders will receive additional training or technical guidance where necessary to enable them to fulfil their responsibilities effectively.

Governor Training

Governors will receive safeguarding training, including online safety, as part of their induction and ongoing professional development.

Training will enable governors to:

- Understand the school's statutory safeguarding responsibilities in relation to online safety.
- Recognise the principal online risks affecting children and the importance of a whole-school approach to online safety.
- Understand the school's filtering and monitoring arrangements and their role in ensuring that these are reviewed and remain effective.
- Understand how online safety is taught through the curriculum and reinforced through the wider school culture.
- Provide appropriate challenge and oversight of the school's arrangements for managing online safety risks.

The Local Governing Body will receive updates on online safety through the school's safeguarding reporting arrangements and will identify any further training needs as appropriate.

Cyberbullying

Cyberbullying is bullying that takes place through digital technology, including social media, messaging platforms, online games and other internet-based services.

Queen Victoria Primary School does not tolerate cyberbullying. We recognise that online bullying can take place both within and outside school and may have a significant impact on pupils' wellbeing, relationships and learning.

The school will:

- Educate pupils about cyberbullying, respectful online communication and the importance of reporting concerns.
- Encourage pupils to report online bullying, whether they are directly involved or have witnessed it.
- Investigate reported incidents in accordance with the school's Behaviour Policy and safeguarding procedures.
- Provide appropriate support for pupils affected by cyberbullying.
- Work with parents and carers, and external agencies where appropriate, to address concerns.

Where cyberbullying takes place outside school but affects pupils' safety, wellbeing or relationships within school, the school will respond in accordance with its safeguarding and behaviour responsibilities.

Parents and carers will be encouraged to discuss the apps, games and websites their children use, who they interact with and healthy boundaries for screen time. Families should follow platform age restrictions and consider a family digital agreement. Useful advice is available through LGfL ParentSafe at parentsafe.lgfl.net and parentonlinesafety.lgfl.net.

Filtering and Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and the Managed Service Provider. The DSL has lead responsibility for safeguarding and online safety, with support from the senior leaders and Managed Service Provider. Day-to-day management of the schools 'managed' infrastructure/network is delegated to the Managed Service Provider. They ensure the school system is as safe and secure as is reasonably possible.

Checks on the filtering and monitoring system are carried out by the Managed Service Provider with involvement of a senior leader.

Filtering

- The school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre.
- Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
- There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective.
- There is a clear process in place to deal with, and log, requests/approvals for filtering changes.
- Filtering logs are regularly reviewed and alert the senior leaders to breaches of the filtering policy, which are then acted upon.
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for staff and children)
- Access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- Monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead or senior leaders; all users are aware that the network and devices are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems using the appropriate blend of strategies informed by the school's risk assessment. These may include:

- Physical monitoring (adult supervision in the classroom)
- Internet use is logged, regularly monitored and reviewed.
- Filtering logs are regularly analysed, and breaches are reported to senior leaders.
- School technical staff regularly monitor and record the activity of users on the school technical systems, when appropriate.

Review of Filtering and Monitoring

The school will undertake a documented review of its filtering and monitoring arrangements at least annually, and following any significant changes to technology, safeguarding risks or school systems.

The review will involve the DSL, senior leaders and the managed service provider.

It will consider:

- Whether filtering and monitoring arrangements remain appropriate for pupils' ages, needs and vulnerabilities.
- Whether harmful and inappropriate content is effectively restricted without unnecessarily limiting teaching and learning.
- Whether monitoring alerts are reviewed and acted upon promptly.
- Whether staff understand their responsibilities for reporting concerns and technical failures.
- Whether appropriate arrangements are in place for all school-managed devices and networks.

Actions arising from the review will be recorded, monitored and reported to governors as appropriate.

The annual review will also involve LGfL and the responsible governor or Trust representative, as appropriate, and consider home and remote-learning arrangements. Regular checks will be documented, including any overblocking, gaps in protection or attempts to bypass safeguards. The review will identify report recipients, urgent escalation routes and cover during staff absence.

Filtering on school-managed devices is provided on site through LGfL WebScreen. Monitoring is provided both on site and off site through Senso, with alerts monitored by the school's Designated Safeguarding Lead (DSL). The school will communicate any limitations in monitoring coverage or alert responses during evenings, weekends, holidays and school closures to relevant users and families.

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements:

- Responsibility for technical security resides with SLT who may delegate activities to identified roles.

- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the managed service provider and will be reviewed, at least annually, by the SLT.
- Password policy and procedures are implemented.
- All users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- All school networks and systems will be protected by secure passwords. Passwords must not be shared with anyone.
- There is a risk-based approach to the allocation of learner usernames and passwords.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems, and cabling are securely located and physical access restricted.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- The managed service provider is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- Personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network.
- Staff members are not permitted to install software, unapproved apps, browser extensions or AI services on a school-owned devices without the consent of the SLT/IT service provider.
- Removable media is not permitted unless approved by the SLT/IT service provider.
- Systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- Mobile device security and management procedures are in place.
- Guest users are provided with appropriate access to school systems based on an identified risk profile.

Approved Platforms and Online Storage

Queen Victoria Primary School uses Arbor, ParentPay and Microsoft Teams. Only school-approved accounts and authorised communication functions may be used for school business. Access to medical and safeguarding information must be restricted to authorised staff. Platforms must have managed accounts, appropriate permissions, retention arrangements and auditable administration.

New applications or platforms with communication facilities, pupil logins or school or pupil data require approval before use and central management. If information is accidentally sent or stored using a private or incorrect account, staff must report this immediately to the headteacher, DSL or DPO, according to the nature of the incident.

Copies of the relevant school and Trust data protection and cyber security policies are available from Lynne Perkins.

Artificial intelligence (AI)

Queen Victoria Primary School recognises that artificial intelligence (AI) offers opportunities to support teaching and learning but also presents potential risks to pupils' safety, privacy and wellbeing.

These risks include exposure to inaccurate or inappropriate information, the sharing of personal data, inappropriate interactions with AI-powered applications and the creation or distribution of misleading or harmful AI-generated content.

The school will:

- Ensure that any AI tools used with pupils are appropriately assessed, authorised and supervised.
- Teach pupils, in an age-appropriate way, that AI-generated information and images may be inaccurate, misleading or manipulated.
- Ensure that pupils do not access generative AI tools independently unless specifically authorised and appropriately supervised.
- Treat the use of AI to bully, intimidate, impersonate or harm others as a serious concern, responding in accordance with safeguarding and behaviour procedures.
- Ensure staff do not enter confidential, sensitive or personally identifiable pupil information into unapproved AI systems. (Pupil photographs, videos and personal information must not be uploaded to unapproved AI tools or online services.)
- Review the risks associated with new AI tools before introducing them into school practice.

Any safeguarding concerns involving AI-generated images, including inappropriate or sexualised images of children, will be referred immediately to the DSL and managed in accordance with safeguarding procedures.

Generative AI Use and Approval

Generative AI use must be carefully managed. Staff using pre-approved tools must use their school account and must not enter personal or sensitive information relating to children, staff or

the school. Users must consider inaccurate, biased or inappropriate output, deepfakes, impersonation and unhealthy interactions with AI chatbots. AI-generated work must not be used to plagiarise or cheat.

Before using any new AI platform, staff must obtain authorisation from Matthew Priest, Headteacher. A Data Protection Impact Assessment (DPIA) must be completed, with advice from Lynne Perkins, the Data Protection Officer (DPO) and Agilisys, as appropriate.

The assessment must consider safeguarding, privacy, security, age restrictions, permitted purposes, supervision and the need for human review of AI-generated content.

Using AI to record or transcribe meetings also requires prior approval and a documented assessment of the privacy and safeguarding implications.

Mobile Devices

Mobile devices may be school owned/provided or personally owned and might include smartphones, tablets, notebooks, laptop or other technology that usually has capability of utilising the school's wireless network. The primary purpose of any use of mobile devices (either school-owned or personal) in school is educational. Any use of mobile devices should be done so in line with other school policies and procedures, including the safeguarding policy, behaviour policy, bullying policy, acceptable use policy and the staff code of conduct.

- The school Acceptable Use Agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies
- The school allows:

	School Devices		Personal Devices		
	School owned for single user	School owned for multiple users	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes *	Yes	Yes
Full network access	Yes	Yes			
Internet only				Yes	Yes
No network access			Yes		

*See *Pupil Mobile Phones and Smart Devices* section below

School-owned devices

- Devices can be used in school to support teaching and learning and can also be taken out of school for work purposes.
- Personal use is not allowed.
- All devices have access to the school internet and are filtered by the school filtering system.
- The managed service provider is responsible for the management of devices, installation of apps and changing of settings and technical support.
- All staff have signed the Acceptable Use Policy.
- School-owned devices are managed by the school's IT service provider and are subject to the school's filtering, monitoring and technical security arrangements. Users are informed that their use of school systems and devices may be monitored in accordance with safeguarding, data protection and acceptable use requirements.
- All devices in school are filtered by LGfL (London Grid for Learning) systems.
- The devices have access to the teachers' one drive account and specific apps that use cloud storage. These must be logged in by the teacher using the device.
- School-managed devices and systems are protected through appropriate technical and organisational security measures, including access controls, password protection, encryption where appropriate, device management and regular security updates. These arrangements support the school's obligations under data protection legislation.
- Taking photos and storing them on devices is allowed for school purposes (for example: evidencing work, blogging). Use of images must follow school policies concerning the sharing, distribution and publication of those images.
- If a teacher leaves the school, the device is given back and wiped so it can be used by a different member of staff.
- Devices are covered by school insurance for accidental damage, fire and theft. If it is lost by a member of staff then they will be responsible for replacing this.
- Staff are given appropriate training to use the devices and are familiar with all the relevant policies regarding use of devices.

Personal devices

- Staff and visitors are allowed to use personal mobile devices in school.
- Mobile phones may only be used in designated areas - in places in school where there are no children present (e.g. offices and the staffroom). Guests devices will be given access specific to the task/activity.
- Devices will not have access to the networks. Staff can have access to the internet, visitors are given access through a 'guest' login.
- No Technical support is available for personal devices.
- Where concerns arise about a pupil's use of a personal electronic device, the school will act in accordance with its Behaviour Policy, safeguarding procedures and current DfE guidance on searching, screening and confiscation. Any search or examination of a device or its contents will be undertaken only where lawful, necessary and proportionate.
- Taking/storage/use of images of children in school is forbidden on personal devices.

- School takes no responsibility for the loss/damage or malfunction following access to the network. However, it is unlikely that any personal devices have access to the network.
- Access to the school internet is only given upon request.
- Pupils are educated about the safe and responsible use of mobile devices as part of Online Safety lessons.

Personal Recording Devices and Wearable Technology

Personal recording devices, including smart glasses, require written permission before being brought into use at school. Secret photography, video or audio recording of pupils or staff, including remotely, is prohibited. Staff must not download pupil or staff data onto private phones.

Staff should keep personal phones on silent and use them only in designated private staff areas. Important personal calls while on duty can be directed through the school office. Volunteers, contractors and governors must not use personal phones in the presence of children or photograph pupils. Any authorised contractor photography of equipment or buildings must have headteacher approval and be supervised by a member of staff.

Pupil Mobile Phones and Smart Devices

Pupils are not permitted to use mobile phones or smart devices with similar communication functionality, including smartwatches, during the school day.

Where pupils are permitted to bring mobile phones to school for travel or safety reasons, these must be switched off and stored securely in accordance with school procedures.

Exceptions may be agreed by the headteacher where necessary to meet individual medical, disability-related or safeguarding needs.

Any misuse of mobile phones or smart devices will be addressed in accordance with the school's Behaviour Policy.

Urgent messages between parents/carers and pupils should be passed through the school office. Parents should seek permission before photographing displays and avoid capturing other children.

Trips and Events Away from School

A school duty phone will be used for authorised and emergency communications during school trips and events. Any necessary deviation must be reported to the headteacher. If a personal phone must be used in an emergency, staff should hide their number to protect professional boundaries. Staff must assess the risks of external Wi-Fi and networks, which may not provide the same filtering and monitoring as school systems, and seek DSL advice where necessary.

Social Media

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- Ensuring that personal information is not published.
- Education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- Clear reporting guidance, including responsibilities, procedures, and sanctions.
- Risk assessment, including legal risk.
- Guidance for learners, parents/carers

For official school social media accounts are established, there should be:

- A process for approval by senior leaders
- Clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff.
- Consideration of the staff code of conduct
- Systems for reporting and dealing with abuse and misuse.
- Understanding of how incidents may be dealt with under school disciplinary procedures.

Where staff use social media professionally or personally:

Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

- No reference should be made in social media to learners, parents/carers or school staff.
- Staff ensure they do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Staff act as positive role models in their use of social media
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

- When parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

Parents/carers and other community members are expected to behave respectfully in public posts and private groups. Confidential information and individual pupil concerns must not be shared through official school social media. Inappropriate or abusive posts may be reported to the platform; support may be sought from the Professionals' Online Safety Helpline and police where appropriate.

Staff, governors, volunteers and contractors must not accept pupil friend requests, follow pupil accounts or communicate privately with pupils through personal social media. Pre-existing family links must be declared and any exception approved by the headteacher. Attempts to establish inappropriate contact must be reported to the DSL or headteacher.

Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying 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 school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press.
- We allow parents/carers to take videos or digital images of their children at school events for personal use. To respect everyone's 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 pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website, particularly in association with photographs.

Before using a pupil's photograph or video, staff must check the latest consent and any safeguarding restrictions. Pupils will be taught about image manipulation, audience, online reputation and the risks of oversharing. Parents must not covertly record interactions at school or share images of other people's children on social media.

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Social media
- Online newsletters

The school website is managed by The Headteacher. The school ensures that the online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.

The school website provides information about online safety e.g., publishing the school's Online Safety Policy and acceptable use agreements; curating latest advice and guidance; an online safety page with appropriate links.

The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process.

Acceptable Use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

Acceptable use agreements

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:

- Staff induction and handbook
- Communication with parents/carers
- Being built into education sessions
- School website

User actions		Acceptable	Acceptable at certain times	Acceptable for Nominated Users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Any illegal activity for example: • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons/firearms offences • Fraud and financial crime including money laundering					X

User actions		Acceptable	Acceptable at certain times	Acceptable for Nominated Users	Unacceptable	Unacceptable and illegal
Users shall not undertake activities that might be classed as cybercrime under the Computer Misuse Act (1990)	- Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) - Gaining unauthorised access to school networks, data and files, through the use of computers/devices - Creating or propagating computer viruses or other harmful files - Revealing or publicising confidential or proprietary information (e.g., financial/personal information, databases, computer/network access codes and passwords) - Disable/Impair/Disrupt network functionality through the use of computers/devices - Using penetration testing equipment (without relevant permission)					X
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)				X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X		
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

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

- When communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
- Any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- Staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community

- Users should immediately report to a nominated person – in accordance with the school 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.

Reporting and Responding to Incidents of Misuse

Queen Victoria Primary School is committed to ensuring that online safety concerns and incidents involving the misuse of technology are identified, reported and responded to promptly, consistently and appropriately.

The school recognises that, despite appropriate safeguarding measures, online safety incidents may occur both within and outside school. These may involve inappropriate online behaviour, cyberbullying, harmful content, inappropriate contact, the misuse of digital devices or online platforms, breaches of data security or suspected illegal activity.

All incidents will be considered in the context of the school's safeguarding responsibilities, with the safety and wellbeing of children remaining the overriding priority.

Reporting Online Safety Concerns

All members of the school community are encouraged to report online safety concerns, including incidents that occur outside school where these may affect pupils' safety, wellbeing or education.

Staff must report any online safety concern involving a pupil to the Designated Safeguarding Lead (DSL) or a deputy DSL without delay, in accordance with the school's safeguarding procedures.

Concerns may include:

- Access to harmful, inappropriate or illegal online content.
- Cyberbullying, harassment, threats or discriminatory behaviour.
- Inappropriate contact, grooming, exploitation or coercion.
- The sharing of personal information, images or videos without consent.
- The creation, sharing or possession of nude or semi-nude images of children, including AI-generated or manipulated imagery.
- Online behaviour that places a pupil or another member of the school community at risk.
- Suspected misuse of school systems, devices or accounts.
- Concerns about data security, unauthorised access or failures in filtering and monitoring systems.

Pupils will be encouraged to speak to a trusted adult if they encounter anything online that makes them feel worried, uncomfortable or unsafe.

Parents and carers should report concerns to the class teacher, DSL or headteacher, as appropriate.

Where a concern involves an immediate risk of harm, staff must take appropriate action to safeguard those involved and seek urgent assistance from the DSL or emergency services where necessary.

Recording and Assessing Incidents

All online safety concerns involving safeguarding risks related to pupils will be recorded on CPOMS in accordance with the school's safeguarding procedures.

Records should include the nature of the concern, relevant information about those involved, actions taken, decisions made and any follow-up required.

The DSL will assess reported safeguarding concerns and determine an appropriate response, taking account of:

- The nature and seriousness of the incident.
- The age, understanding and vulnerability of the pupils involved.
- Whether there is a risk of harm, abuse or exploitation.
- Whether the incident may involve criminal activity.
- Whether other pupils or members of the school community may be affected.
- Whether parents/carers or external agencies should be involved.

The DSL will ensure that safeguarding concerns are responded to promptly and that appropriate support is provided to those affected.

Responding to Incidents

The school's response will be proportionate to the circumstances and will distinguish between safeguarding concerns, inappropriate behaviour, technical misuse and suspected criminal activity.

Where incidents involve inappropriate online behaviour, such as cyberbullying or misuse of school technology, they will be addressed in accordance with the school's Behaviour Policy and Anti-Bullying Policy, alongside any necessary safeguarding response.

Actions may include:

- Providing support and reassurance to pupils affected by an incident.
- Working with parents and carers, where appropriate.
- Providing additional online safety education or targeted intervention.
- Applying appropriate consequences in accordance with the Behaviour Policy.
- Reviewing supervision, access to technology or relevant technical safeguards.
- Seeking advice or support from external agencies where necessary.

Behavioural consequences will not replace appropriate safeguarding action. The school recognises that pupils involved in harmful online behaviour may themselves require safeguarding support.

Where incidents occur outside school but affect pupils or the school community, the school will respond within its safeguarding and behaviour responsibilities, working with parents/carers and other agencies where appropriate.

Incidents Involving Nude or Semi-Nude Images of Children

Any incident involving the creation, possession, sharing or threatened sharing of nude or semi-nude images of children, including AI-generated or manipulated sexual imagery, must be reported immediately to the DSL.

Staff must not intentionally view, copy, print, share, store or save such imagery, or ask a pupil to download, forward or share it. Staff must not delete the imagery or instruct a pupil to delete it before the DSL has assessed the concern.

If imagery is viewed accidentally, staff must report this immediately to the DSL and explain the circumstances.

The DSL will assess the incident in accordance with current UKCIS guidance on sharing nude and semi-nude images and the school's safeguarding procedures. This will include consideration of the pupils' ages, the circumstances in which the imagery was created or shared, any coercion or exploitation, and whether referrals to children's social care or the police are required.

Decisions about viewing imagery in exceptional circumstances, preserving evidence, reporting content or arranging its removal will be made by the DSL in accordance with relevant guidance and, where necessary, advice from appropriate agencies.

The school will provide appropriate support to pupils affected by such incidents, taking care to avoid unnecessary distress, blame or further sharing of the imagery.

Suspected Illegal Activity and Serious Safeguarding Concerns

Where an online safety incident involves suspected criminal activity or a risk of significant harm, the DSL will ensure that the concern is escalated through the school's safeguarding procedures. This may include incidents involving child sexual abuse material, grooming, exploitation, threats, harassment, extortion, hate crime, radicalisation or serious cybercrime.

Where appropriate, the DSL will seek advice from or make referrals to children's social care, the police, CEOP or other relevant agencies.

Staff must not undertake their own investigation into suspected illegal material or attempt to access, download, copy or distribute potentially unlawful content.

Any relevant devices, accounts or digital evidence will be managed in accordance with safeguarding procedures and advice from the appropriate authorities. Staff must not interfere with or delete potential evidence without appropriate advice.

Where a child is at immediate risk of harm, the police or emergency services will be contacted without delay.

Technical Misuse and Security Incidents

Concerns involving the misuse of school devices, networks, accounts or digital systems must be reported promptly to the appropriate senior leader and, where necessary, the managed IT service provider. This includes suspected unauthorised access, attempts to bypass filtering and monitoring systems, malware, compromised accounts, inappropriate use of school technology and potential data security breaches.

The school will work with its managed IT service provider and relevant trust personnel to investigate technical concerns, secure affected systems and identify any necessary corrective action. Where a technical incident also presents a safeguarding concern, the DSL must be informed immediately. Suspected personal data breaches will be managed in accordance with the trust's Data Protection Policy and relevant reporting procedures.

Concerns Involving Staff

Concerns about the inappropriate or unsafe use of technology by a member of staff, volunteer or contractor must be reported to the headteacher. Where a concern involves the headteacher, it must be reported to the Chief Executive Officer of Stour Vale Academy Trust in accordance with the trust's safeguarding and managing allegations procedures.

Concerns involving staff will be managed in accordance with the school's Child Protection and Safeguarding Policy, Staff Code of Conduct and relevant trust procedures.

Where a concern may meet the threshold for an allegation against an adult working with children, the school will follow the appropriate procedures, including consultation with the Local Authority Designated Officer (LADO) where required.

Lower-level concerns will be addressed in accordance with the school's safeguarding and staff conduct arrangements.

Staff must not conduct informal investigations into allegations involving colleagues or attempt to access potentially unlawful material.

Supporting Those Involved

The school recognises that online safety incidents can have a significant impact on children's emotional wellbeing, relationships and sense of safety.

Appropriate support will be provided to pupils affected by incidents, including those who have reported concerns, experienced harm or been involved in harmful online behaviour.

The school will work with parents and carers wherever appropriate, taking account of safeguarding considerations and the need to protect children from further harm.

Information about incidents and their outcomes will be shared only with those who have a legitimate need to know, in accordance with safeguarding and data protection requirements.

Additional Safeguarding Concerns

Upskirting, including the use of discreet recording technology, will be treated as a safeguarding concern and managed under the school's child-on-child abuse procedures. Staff must not dismiss harmful behaviour as banter. Concerns about extremist material, radicalisation or hate speech must be reported through safeguarding and Prevent procedures.

The school may seek support from children's services, police, NCA CEOP, the Internet Watch Foundation, the Prevent team, LGfL and the UK Safer Internet Centre's Professionals' Online Safety Helpline, according to the concern.

Reviewing Incidents and Learning from Concerns

The DSL and senior leaders will review online safety incidents and patterns of concern to identify any necessary improvements to safeguarding arrangements, teaching, supervision or technical security.

Learning from incidents may inform:

- Updates to the online safety curriculum and targeted pupil support.
- Staff training and safeguarding briefings.
- Reviews of filtering, monitoring and technical security arrangements.
- Communication and guidance for parents and carers.
- Updates to relevant school policies and procedures.

Significant incidents, emerging risks and relevant trends will be reported to the Local Governing Body through the school's safeguarding reporting arrangements, without disclosing unnecessary personal information.

The school will ensure that its procedures for reporting and responding to online safety incidents remain consistent with current statutory guidance and the safeguarding arrangements of Stour Vale Academy Trust.

Responding to Pupil Actions

	Refer to class teacher	Refer to AHT/DHT/DSL	Refer to Headteacher	Refer to police/ social care	Refer to Agilisys/LGfL technical support for advice or action	Inform parents/carers	Remove device/network access rights	Issue a warning	Further sanction in line with behaviour policy
--	------------------------	----------------------	----------------------	---------------------------------	---	-----------------------	--	-----------------	---

Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X	X	X					
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords	X	X	X						
Corrupting or destroying the data of other users.	X	X	X					X	
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X		X	
Unauthorised downloading or uploading of files or use of file sharing.	X	X	X						
Using proxy sites or other means to subvert the school's filtering system.	X	X	X			X		X	
Accidentally accessing offensive or pornographic material and failing to report the incident.	X	X	X			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	X	X			X			
Unauthorised use of digital devices (including taking images)	X								
Unauthorised use of online services	X								
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X	X	X			X			
Continued infringements of the above, following previous warnings or sanctions.	X	X	X			X	X		X

Responding to Staff Actions

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure

Supporting Guidance

LGfL online safety policy templates: <https://safepolicies.lgfl.net/>

LGfL online safety audit: <https://onlinesafetyaudit.lgfl.net/>

LGfL resources for staff: <https://saferesources.lgfl.net/>

UKCIS guidance on sharing nudes and semi-nudes and the school's relevant safeguarding procedures should be used when responding to intimate imagery concerns.

GDPR Personal Data

This policy adheres to the principles under data protection law. For further information please review the school's data protection policy published on the school's website.

School and Provider Details to Confirm

Before approval, confirm the named DSL and deputies, computing and PSHE leads, responsible governor or Trust representative and DPO contact arrangements. Review anonymised local online safety trends and the annual audit to identify priorities.

Agilisys and LGfL should confirm filtering and monitoring product names, device and user coverage on and off site, Safe Search and YouTube controls, permitted search engines, check frequency and record location, monitoring report recipients, review frequency, urgent response arrangements and absence cover. SchoolProtect, HomeProtect and Senso were mentioned in the LGfL template; their deployment at Queen Victoria has not been confirmed.

Confirm approved platform functions, administration and retention arrangements; image storage, access and retention; website hosting and day-to-day administration; official social media accounts and administrators; and permitted staff AI tools, purposes, training and meeting recording rules.

Confirm whether CCTV is used and, if so, its purpose, lawful basis, access controls, retention period, privacy notices and applicable policy. Confirm the proposed restriction on AirTags and similar tracking devices, including trip arrangements, before adopting it. The existing pupil phone and smartwatch rules and personal image restrictions remain as set out in this policy.

Pupil Acceptable Use Agreements are intended to ensure that:

- Young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use
- School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *students/pupils* to agree to be responsible users

EYFS & KS1 Acceptable Use Agreement

Queen Victoria Primary School – Acceptable Use Agreement (AUA for Children)

When I log on I agree that:

Queen Victoria Primary School – Acceptable Use Agreement (AUA for Children)

When I log on I agree that:



I will only use my own username and password to log on. I will keep my password secret.



I will only use websites that have been suggested by the teacher or a grown up.



I will not give out personal information; tell people where I live, my phone number or where I go to school without permission from the teacher/parent.



I will always ask an adult before sharing photos. I will only share photos that I don't mind everyone seeing.



I will tell a grown up if I feel scared, unsafe, worried or unhappy about anything I find when using the school computers/laptops.



I will respect school property; I will use the internet, computers and laptops and all other equipment properly.

Primary Pupil AUA

Queen Victoria Primary School –

Rules for Responsible Internet Use for Primary Pupils

The school has installed computers and provided Internet access to help our learning. I understand that the school may check my computer files and may monitor any Internet sites I visit.

These rules will keep everyone safe and help us to be fair to others. It is important that you read this policy carefully. If there is anything that you do not understand, please ask.

I agree that:

I will not share any of my passwords with anyone, or use another person's password. If I find out someone else's password, I will tell that person and a member of the school staff, so they can change it.

I will use a password which contains some small and some big (capital) letters plus a number or a symbol *e.g. Skool5 or com**2er* and change it on a regular basis.

I will use the technology at school for learning. I will use the equipment properly and not interfere, change or delete someone else's work.

If I use a flash drive or other storage device, I will follow school guidelines on their use.

I will only e-mail people I know, or my teacher has approved.

If I attach a file to an email, it will not include any inappropriate materials (something I would not want my teacher to see or read) or anything that threatens the integrity of the school ICT system.

I will be respectful in how I talk to and work with others online and never write or participate in online bullying. If anyone sends me a message, I do not like or feel uncomfortable about I will show it to my teacher or parent.

I will report any unpleasant material or messages sent to me. I understand my report would be confidential and would help protect other pupils and myself.

I will not download any programmes or games on to the school computers, netbooks or laptops unless I have permission to do so.

I will always check with a responsible adult before I share or publish images of myself, my friends or other people onto the internet.

I will not make audio or video recordings of another pupil or teacher without their permission.

When using sites on the internet, I will not give my name, home address, telephone/mobile number, pretend to be someone else or arrange to meet someone I do not know, unless my parent, carer or teacher has given permission.

I will always follow the 'terms and conditions' when using a site. The content on the web is someone's property and I will ask my teacher to help me get permission if I want to use information, pictures, video, music or sound files.

I will think carefully about what I read on the Internet, question if it is from a reliable source and use the information to help me answer any questions (I should not copy and paste the information and say it's my own work).

If I want to connect my own device to the school network, I will check with my teacher to see if it is possible.

I am aware of the CEOP report button and know when to use it.

I know anything I do on the computer may be seen by someone else.

Signed:

PRINT NAME:

Dated:

Staff Guardianship Loan Form

Queen Victoria Primary School – Portable ICT Equipment – Staff Guardianship Loan Form

Name has permission to loan and is guardian of the following item(s)
of ICT equipment: -

Item	Serial No	Start date	Return date

Whilst the above items are in your care, the school will expect you to take full personal responsibility for the safe custody of all of the items listed and to follow the guidelines below: -

- I will ensure the mobile device is secured or locked away when not in use;
- I will ensure that unauthorised software is not loaded or run on this mobile device;
- I will not download, store or collect any inappropriate material on the device
- I will ensure that all external media sources (discs, USB flash drives/memory sticks) are checked for viruses before data transfer to the mobile device where appropriate;
- I will ensure the device is regularly virus-checked where appropriate;
- I will ensure the Anti-virus- software, where appropriate, is kept up to date;
- I will ensure that data remains confidential and secure;
- Where personal data about staff or pupils, or school confidential data, is stored on the device, the device will be encrypted and password protected (as appropriate to the device), and the data will be removed as soon as reasonably possible
- I will ensure that the equipment is not used by anyone who has not been authorised by the school
- I will return the device upon request and when I am on leave or other absence, unless otherwise authorised.
- I will ensure the equipment is not left unattended in any vehicle (as this is not covered by the school's insurance policy), and accept that any loss arising from a loss from a vehicle will be my own responsibility.
- If the equipment is lost or stolen, I will inform the police as soon as possible to get a crime number and also contact the appropriate member of staff

Signed

Date

Name person authorising the loan

Signed

Date

Pupil Guardianship Loan Form

Queen Victoria Primary School – Portable ICT Equipment – Pupil Guardianship Loan Form

Name has permission to loan and is guardian of the following item(s) of ICT equipment: -

Item	Serial No	Start date	Return date

Whilst the above item is in your care, the school will expect you to take full personal responsibility for the safe custody of this item and to follow the guidelines below: -

- I will look after the device. I will ensure it is secured or locked away when not in use;
- I agree to use it sensibly. I will ensure that unauthorised software is not loaded or run on this mobile device;
- I will not download, store or collect any inappropriate material on the device
- I will ensure that all external media sources (discs, USB flash drives/memory sticks) are checked for viruses before data transfer to the mobile device where appropriate;
- I will ensure the device is regularly virus-checked where appropriate;
- I will ensure that data remains confidential and secure;
- Any personal data stored on the device will be encrypted if appropriate and removed as soon as reasonably possible
- I will ensure that the equipment is not used by anyone who has not been authorised by the school
- I will return the device upon request and when I am on leave or other absence, unless otherwise authorised.
- I will ensure the equipment is not left unattended in any vehicle (as this is not covered by the school's insurance policy), and accept that any loss arising from a loss from a vehicle will be my own responsibility.
- If the equipment is lost or stolen, I will inform the police as soon as possible to get a crime number and also contact the appropriate member of staff

Parents' Consent Form

I give permission for my son/daughter (Name)
to receive a for the duration of the project.
Signed (Parent/Carer)

Name person authorising the loan

Signed Date