University Schools Trust
A transformational education

Cyril Jackson School
Part of University Schools Trust
Inspiring Minds Through Opportunity

Online Safety Policy

September 2026

Title:	Online Safety Policy
Source:	CJPS
Document Owner:	Yessica Gimenez
Review & Update By:	Yessica Gimenez
Advisory Committee:	CJPS Committee
Approval Committee:	CJPS Committee
Date Approved:	September 2026
Date of Publication:	September 2027
Date of Next Review:	September 2027
Required on Website:	Yes

0. Document Control

The table below contains the changes made between the different final editions of this document set for approval. This is to help provide information to those reviewing and approving the document of the changes being made.

Document Edition	Section	Details of change
September 2024	All	Reformatting
	3	Updated "legislation and guidance"
	4	Updated "roles and responsibilities"
	8	Updated "child on child sexual abuse and harassment"
September 2025	All	Change of date
September 2026	All	This policy has been comprehensively reviewed and updated to reflect the latest statutory guidance and best practice, including Keeping Children Safe in Education (September 2026), the Department for Education's Filtering and Monitoring Standards for Schools and Colleges, UK Council for Internet Safety (UKCIS) guidance and relevant data protection legislation. Updates include strengthened governance and safeguarding arrangements, enhanced guidance on filtering and monitoring, artificial intelligence (AI), cyber security, emerging online risks, digital resilience and media literacy. Sections have been restructured to improve clarity, reduce duplication with other school policies and strengthen cross-references to the Child Protection and Safeguarding Policy, Data Protection Policy, Cyber Security Policy and other related procedures. Additional content has been included to reflect current expectations regarding educational technology, approved digital platforms, remote learning and staff, pupil and parent responsibilities in maintaining a safe online environment.

Contents

0. Document Control 3
1. Definitions 5
2. Scope of the Policy 5
3. Links to Legislation and Guidance Documents 6
4. Roles and Responsibilities 7
5. Managing Online Safety 10
6. Handling Online Safety Concerns 10
7. Cyberbullying 11
8. Child-On-Child Sexual Abuse and Harassment 12
9. Grooming and Exploitation 13
10. Child Sexual Exploitation (CSE) and criminal exploitation (CCE) 13
11. Radicalisation 14
12. Mental Health 15
13. Online Hoaxes and Harmful Online Challenges 15
14. Cyber Crime 16
15. Online Safety Training for Staff 17
16. Online Safety and the Curriculum 17
17. The Use of Technology in the Classroom 18
18. Use of Smart Technology 19
19. Educating Parents 19
20. Internet Access 20
21. Filtering and Monitoring Systems 21
22. Network Security 23
23. Emails 24
24. Generative AI 25
25. Social Networking 26
26. The School Website 26
27. Use of Devices 27
28. Remote Learning 27
29. Protecting Personal Information 28
30. Educational Apps and Third-Party Platforms 28

1. Definitions

The "Trust" refers to the company known as the University Schools Trust, East London and all Trustees, Governors and Staff who work within it.

"The school" refers to an individual academy within the Trust, as denoted by their Unique Reference Number. As such a 'school' may span one or several phases of education to the individual academies within the Trust. Depending on the context the term "School" may refer to a singular academy or to all of the academies within the Trust but as separate entities.

"Online Safety" refers to the safe, responsible and appropriate use of digital technologies, online services and the internet. It encompasses safeguarding children and staff from online risks relating to content, contact, conduct and commerce, as well as promoting positive digital citizenship.

"Filtering" refers to the systems and controls implemented to restrict access to illegal, inappropriate or harmful online content in accordance with the Department for Education's Filtering and Monitoring Standards.

"Monitoring" refers to the processes and technologies used to identify and respond to safeguarding concerns arising from the use of the school's digital systems and online services.

"Generative Artificial Intelligence (Generative AI)" refers to technology capable of generating text, images, audio, video, code or other content in response to user prompts.

2. Scope of the Policy

Cyril Jackson Primary School recognises that digital technologies and online services play a vital role in education, communication and everyday life. The school is committed to promoting a culture of online safety that enables pupils, staff and the wider school community to use technology safely, responsibly and confidently whilst protecting them from online harm.

Online safety is recognised as an integral part of the school's safeguarding responsibilities and is embedded throughout the curriculum, staff training, policies, procedures and the wider school culture.

The school recognises that online risks continue to evolve alongside technological developments, including the increasing use of social media, mobile technologies and artificial intelligence (AI). The school will regularly review its approach to online safety to ensure it remains effective, proportionate and reflective of current statutory guidance and emerging risks.

The breadth of issues classified within online safety is considerable; however, they can be categorised into four areas of risk:

Content – Being exposed to illegal, inappropriate or harmful material, e.g. pornography, misinformation and disinformation (including fake news), self-harm and suicide content, discriminatory content, extremist material and AI-generated harmful content.

Contact – Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, adults posing as children or young people, grooming, coercion, exploitation and financial scams.

Conduct – Personal online behaviour that increases the likelihood of, or causes, harm, e.g. cyberbullying, the sharing of explicit images, inappropriate online behaviour and the misuse of digital technologies.

Commerce – Risks associated with online gambling, phishing, fraud, financial scams, malicious advertising and other forms of online exploitation.

The measures implemented by the school to protect pupils, staff and visitors are designed to address each of these areas of risk. This policy provides the framework for promoting online safety, preventing harm and responding appropriately to online safety concerns across the school community.

3. Links to Legislation and Guidance Documents

3.1. Relevant Internal Documents

This policy should be read in conjunction with the following policies and documents.

- Social Media Policy
- Allegations of Abuse Against Staff Policy
- Technology Acceptable Use Agreement
- Cyber-security Policy
- Cyber Response and Recovery Plan
- Child Protection and Safeguarding Policy
- Child-on-child Abuse Policy
- Anti-Bullying Policy
- Pupils' Personal Electronic Devices Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedure
- Data Protection Policy
- Confidentiality Policy
- Photography and Images Policy
- Device User Agreement
- Staff ICT and Electronic Devices Policy
- Prevent Duty Policy
- Remote Education Policy
- Home School Agreement
- SEND Policy
- Social, Emotional and Mental Health Policy

3.2. Relevant External Documents

Relevant external documents to refer to are the:

- Data Protection Act 2018
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2022) 'Searching, screening and confiscation'
- Online Safety Act 2023
- DfE (2023) 'Generative artificial intelligence in education'
- DfE (2023) 'Teaching online safety in school'
- DfE (2024) 'Filtering and monitoring standards for schools and colleges'
- Department for Science, Innovation and Technology and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE (2026) 'Keeping children safe in education'
- Meeting Digital and Technology Standards for Schools and Colleges
- Generative AI: Product Safety Expectations
- UK Council for Internet Safety – Education for a Connected World
- UK Safer Internet Centre – Appropriate Filtering and Monitoring Guidance
- National Cyber Security Centre – Cyber Security Standards for Schools and Colleges

4. Roles and Responsibilities

4.1. Trust

The Trust is responsible for:

- Ensuring this policy complies with relevant legislation, statutory guidance and Trust requirements.
- Seeking assurance that effective online safety arrangements, including filtering and monitoring systems, are in place and operating effectively.
- Ensuring sufficient resources are available to support effective online safety, safeguarding and cyber security arrangements.
- Ensuring online safety remains an integral part of the Trust's safeguarding arrangements.
- Ensuring staff receive appropriate safeguarding and online safety training, including training on filtering and monitoring, as part of induction and regular safeguarding updates.

4.2. Governing Board / School Committee

The School Committee is responsible for:

- Reviewing and approving this policy.
- Monitoring the implementation and effectiveness of the school's online safety arrangements.
- Seeking assurance that appropriate filtering and monitoring systems remain effective and are reviewed at least annually.
- Receiving assurance regarding significant online safety incidents, emerging risks and actions taken to promote continuous improvement.

4.3. Headteacher

The headteacher is responsible for:

- Ensuring this policy is implemented consistently throughout the school.
- Promoting a whole-school culture of online safety.
- Ensuring online safety remains an interrelated theme across safeguarding, behaviour, curriculum and staff conduct.
- Ensuring appropriate filtering and monitoring arrangements are in place and reviewed regularly.
- Ensuring staff receive appropriate online safety training and safeguarding updates.
- Ensuring sufficient resources are available to support effective online safety arrangements.
- Supporting the DSL by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Reporting significant online safety matters to the Trust and School Committee, where appropriate.

4.4. DSL

At Cyril Jackson, the DSL is the headteacher, however the headteacher may delegate some responsibilibities to the deputy DSL's. These responsibilities include:

- Taking the operational lead for online safety and online safeguarding.
- Ensuring online safety is embedded within the school's safeguarding arrangements.
- Understanding the filtering and monitoring systems in place and responding appropriately to safeguarding concerns identified through those systems.
- Liaising with the ICT provider, Trust, external agencies and safeguarding partners where appropriate.
- Ensuring online safety concerns are managed in accordance with the Child Protection and Safeguarding Policy.
- Ensuring all online safety concerns are appropriately recorded on CPOMS.
- Monitoring online safety incidents to identify trends, emerging risks and training needs.
- Providing safeguarding and online safety updates to staff.
- Reviewing online safety risks and supporting the annual review of this policy.

4.5. Finance & Statutory Compliance Manager

The Finance & Statutory Compliance Manager is responsible for:

- Supporting the Headteacher in ensuring compliance with relevant online safety legislation and statutory guidance.
- Coordinating the annual review of filtering and monitoring arrangements in conjunction with the DSL and ICT provider.
- Supporting the procurement and implementation of secure digital systems.
- Maintaining records relating to online safety audits, compliance reviews and statutory requirements.
- Monitoring compliance with the DfE Filtering and Monitoring Standards.
- Supporting the continuous improvement of the school's online safety arrangements.

4.6. ICT Provider

The ICT Technician is responsible for:

- Implementing and maintaining appropriate filtering and monitoring systems.
- Maintaining the security and integrity of the school's network, systems and devices.

- Applying software updates, security patches and cyber security measures.
- Investigating technical issues relating to filtering, monitoring or cyber security.
- Supporting safeguarding investigations where technical information is required.
- Reporting any safeguarding concerns identified through technical monitoring to the DSL immediately.

4.7. Staff

Staff are responsible for:

- Maintaining an awareness of current online safety risks and safeguarding concerns.
- Promoting the safe, responsible and appropriate use of technology.
- Modelling positive online behaviour and maintaining appropriate professional boundaries.
- Following this policy and all associated acceptable use agreements.
- Reporting online safety concerns to the DSL without delay and recording safeguarding concerns on CPOMS in accordance with the Child Protection and Safeguarding Policy.
- Participating in mandatory online safety and safeguarding training.
- Escalating concerns relating to filtering or monitoring systems where appropriate.

4.8. Parents

Parents are responsible for:

- Supporting the school's approach to online safety.
- Reinforcing safe and responsible online behaviour at home.
- Monitoring and supporting their child's use of technology, where appropriate.
- Reporting online safety concerns to the school promptly.
- Supporting the school's Acceptable Use Agreements and reinforcing age restrictions for online services and social media platforms.

4.9. Pupils

Pupils are responsible for:

- Using technology safely, responsibly and respectfully.
- Following the school's Acceptable Use Agreements.
- Respecting the privacy and wellbeing of others when using technology.
- Reporting anything seen or experienced online that causes concern to a trusted adult immediately.
- Keeping passwords secure and not attempting to bypass the school's filtering or monitoring systems.

4.10. Visitors and Contractors

Visitors and contractors are responsible for:

- Complying with this policy whilst on the school site or when using school systems.
- Using school technology appropriately and only for authorised purposes.
- Reporting safeguarding or online safety concerns immediately to a member of staff.
- Following the school's Acceptable Use Agreement where applicable.

5. Managing Online Safety

Online safety is recognised as an integral part of the school's safeguarding responsibilities. The school adopts a whole-school approach to online safety, ensuring that safeguarding considerations are embedded across leadership, governance, curriculum, staff training, technology, filtering and monitoring arrangements, behaviour management and engagement with parents and carers.

The Designated Safeguarding Lead (DSL) has operational responsibility for online safety and will work closely with the Headteacher, Finance & Statutory Compliance Manager, ICT Provider and other relevant staff to ensure effective online safety arrangements are maintained.

The school recognises that technology is a significant factor in many safeguarding concerns and that online risks continue to evolve. The school will regularly review its approach to online safety to ensure it remains effective, proportionate and reflective of current statutory guidance, emerging technologies and safeguarding risks.

The school promotes online safety by:

- Embedding online safety throughout the curriculum in an age-appropriate manner.
- Providing regular safeguarding and online safety training for staff.
- Delivering online safety education through lessons, assemblies and wider enrichment opportunities.
- Maintaining appropriate filtering and monitoring systems in accordance with the DfE Filtering and Monitoring Standards.
- Promoting positive digital citizenship and responsible use of technology.
- Working in partnership with parents and carers to support online safety beyond the school environment.
- Responding promptly and proportionately to online safety concerns in accordance with the Child Protection and Safeguarding Policy.
- Regularly reviewing emerging online risks, including those associated with artificial intelligence, social media, gaming platforms and new technologies.

The school recognises that some pupils may be more vulnerable to online harm than others, including pupils with SEND, those with identified safeguarding needs and those who may require additional support to understand and manage online risks. Appropriate support and education will be provided in accordance with individual needs.

6. Handling Online Safety Concerns

All online safety concerns will be treated as safeguarding concerns where there is a risk of harm to a pupil. Concerns will be managed in accordance with the school's Child Protection and Safeguarding Policy and recorded on CPOMS, where appropriate.

Staff will respond to online safety concerns promptly, proportionately and without judgement, recognising that online harm can have a significant impact on a pupil's safety, wellbeing and mental health.

Where a pupil discloses that they have experienced online abuse, exploitation, harassment or any other form of online harm, staff will:

- Listen carefully and reassure the pupil that they have done the right thing by speaking to a trusted adult.
- Avoid asking leading questions or promising confidentiality.
- Make an accurate record of the concern as soon as possible.
- Report the concern immediately to the Designated Safeguarding Lead (DSL).
- Record the concern on CPOMS in accordance with the Child Protection and Safeguarding Policy.

The DSL will assess each concern on an individual basis, taking account of the nature of the incident, the level of risk, the needs of the pupil and any wider safeguarding concerns. Where appropriate, referrals will be made to children's social care, the police or other relevant agencies in accordance with statutory safeguarding procedures.

The school recognises that online abuse and harmful online behaviour often occur alongside other safeguarding concerns. All online safety concerns will therefore be considered within the wider safeguarding context, including any known vulnerabilities, previous concerns or patterns of behaviour.

Where online safety concerns involve child-on-child abuse, harmful sexual behaviour, exploitation, cyberbullying, radicalisation or criminal activity, they will be managed in accordance with the relevant sections of this policy and the Child Protection and Safeguarding Policy.

The school recognises that pupils who display harmful online behaviour may themselves be vulnerable or have experienced abuse. Appropriate safeguarding support and intervention will therefore be considered for all pupils involved.

Where appropriate, the school will preserve relevant evidence relating to online safety incidents, such as screenshots, URLs or device information, in accordance with safeguarding procedures and advice from the police or other relevant agencies.

7. Cyberbullying

The school recognises that cyberbullying is a form of bullying and will not be tolerated under any circumstances. Cyberbullying will be managed in accordance with the Behaviour Policy, Anti-Bullying Policy and Child Protection and Safeguarding Policy, where appropriate.

Cyberbullying is the use of technology or online platforms to intentionally and repeatedly cause harm, distress or humiliation to another person. It may occur through social media, messaging applications, gaming platforms, online forums, email, websites or any other digital communication platform.

Cyberbullying may include, but is not limited to:

- Sending abusive, threatening or offensive messages.
- Sharing embarrassing, humiliating or inappropriate images or videos.
- Deliberately excluding individuals from online groups or activities.
- Creating or sharing fake profiles or impersonating another person.

- Posting or sharing harmful, false or malicious information.
- Encouraging others to target, intimidate or harass an individual online.
- Sharing personal information without consent.

All reports of cyberbullying will be taken seriously and investigated promptly. The school will provide appropriate support to pupils affected by cyberbullying and implement proportionate measures to address the behaviour in accordance with the Behaviour Policy.

Where cyberbullying involves safeguarding concerns, child-on-child abuse, discrimination, harassment, exploitation or criminal offences, the matter will be managed in accordance with the Child Protection and Safeguarding Policy and, where appropriate, referred to external agencies.

The school recognises that incidents of cyberbullying may occur outside school; however, where such behaviour affects the safety, wellbeing or education of pupils, or has the potential to disrupt the orderly running of the school, appropriate action will be taken.

Online safety education, positive digital citizenship and respectful online behaviour are promoted throughout the curriculum to reduce the risk of cyberbullying and encourage pupils to report concerns promptly.

8. Child-On-Child Sexual Abuse and Harassment

The school recognises that child-on-child sexual abuse and harassment can occur both online and offline and will not be tolerated under any circumstances. All incidents will be taken seriously and managed in accordance with the Child Protection and Safeguarding Policy, the Behaviour Policy and current statutory guidance.

Online child-on-child abuse may include, but is not limited to:

- The non-consensual sharing of nude or semi-nude images or videos.
- Sexual harassment through social media, messaging services, gaming platforms or other online communication.
- Sexualised comments, unwanted sexual messages or inappropriate online behaviour.
- The creation, sharing or distribution of manipulated, altered or AI-generated sexual images.
- Coercion, intimidation or pressure to create or share sexual content.
- Online exploitation or abuse facilitated by digital technologies.

Staff will maintain an attitude of 'it could happen here' and will respond promptly to all concerns, recognising that online child-on-child abuse may be an indicator of wider safeguarding concerns.

All concerns will be reported immediately to the Designated Safeguarding Lead (DSL) and recorded on CPOMS in accordance with the Child Protection and Safeguarding Policy.

The wishes of the victim will be considered wherever possible; however, the school will always act in the best interests of the child and in accordance with its safeguarding responsibilities. Appropriate support will be provided to all pupils involved, recognising that pupils displaying harmful behaviour may themselves require safeguarding intervention.

Where appropriate, the school will work in partnership with parents, children's social care, the police and other relevant agencies to safeguard pupils and manage identified risks.

9. Grooming and Exploitation

The school recognises that children may be at risk of grooming and exploitation through online platforms, including social media, gaming platforms, messaging applications, live streaming services and other digital technologies. Grooming may be carried out by adults or, in some circumstances, by other children.

Online grooming is a process through which an individual seeks to establish trust or an emotional connection with a child in order to manipulate, exploit or abuse them. This may include sexual abuse, criminal exploitation, financial exploitation, radicalisation or other forms of harm.

Staff will maintain an attitude of 'it could happen here' and will remain vigilant to indicators that a pupil may be experiencing online grooming or exploitation. Concerns will always be considered within the wider safeguarding context and managed in accordance with the Child Protection and Safeguarding Policy.

Potential indicators may include, but are not limited to:

- Becoming secretive or anxious about online activity.
- Receiving gifts, money or new possessions that cannot be explained.
- Spending increasing amounts of time communicating online with unknown individuals.
- Displaying sudden changes in behaviour, mood or emotional wellbeing.
- Using multiple accounts, devices or applications to conceal online activity.
- Becoming reluctant to discuss online relationships or contacts.

Any concerns relating to online grooming or exploitation will be reported immediately to the Designated Safeguarding Lead (DSL) and recorded on CPOMS in accordance with the Child Protection and Safeguarding Policy.

Where appropriate, the DSL will work with children's social care, the police and other relevant agencies to safeguard the child and manage identified risks.

The school recognises that emerging technologies, including artificial intelligence, anonymous messaging platforms and encrypted communication services, may increase opportunities for online grooming and exploitation. Staff training and online safety education will therefore be reviewed regularly to reflect emerging risks.

10. Child Sexual Exploitation (CSE) and criminal exploitation (CCE)

The school recognises that children may be at risk of both Child Sexual Exploitation (CSE) and Child Criminal Exploitation (CCE), including where exploitation is facilitated through online platforms and digital technologies.

Child Sexual Exploitation (CSE) is a form of child sexual abuse in which an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child into sexual activity in exchange for something the child needs or wants, or for the financial or other advantage of the perpetrator.

Child Criminal Exploitation (CCE) occurs where an individual or group manipulates, coerces or deceives a child into criminal activity for the benefit of others. This may include, but is not limited to, county lines activity, drug distribution, theft, financial crime or other forms of criminal exploitation.

The school recognises that online technologies may be used to groom, recruit, manipulate or control children for the purposes of CSE or CCE through social media, messaging applications, gaming platforms, live streaming services or other online environments.

Staff will maintain an attitude of 'it could happen here' and remain vigilant to indicators of exploitation. Concerns will always be considered within the wider safeguarding context and managed in accordance with the Child Protection and Safeguarding Policy.

Any concerns relating to Child Sexual Exploitation or Child Criminal Exploitation will be reported immediately to the Designated Safeguarding Lead (DSL) and recorded on CPOMS in accordance with the Child Protection and Safeguarding Policy.

Where appropriate, the DSL will work in partnership with children's social care, the police and other relevant agencies to safeguard the child and manage identified risks.

11. Radicalisation

The school recognises that the internet, social media, online forums, gaming platforms and other digital technologies may be used to promote extremist views, radicalise individuals and encourage involvement in terrorism or other forms of harmful ideology.

Radicalisation is the process by which an individual comes to support terrorism or extremist ideologies associated with terrorist groups. Children may be exposed to extremist material online through deliberate targeting, online grooming, social media algorithms, online communities or by accessing harmful content.

The school recognises that online radicalisation is a safeguarding concern and will respond to concerns in accordance with the Child Protection and Safeguarding Policy and Prevent Duty guidance.

Staff will maintain an attitude of 'it could happen here' and remain vigilant to indicators that a pupil may be vulnerable to radicalisation or extremist influence.

Any concerns relating to radicalisation or extremist content will be reported immediately to the Designated Safeguarding Lead (DSL) and recorded on CPOMS in accordance with the Child Protection and Safeguarding Policy.

Where appropriate, the DSL will work with the Local Authority, Police, Children's Social Care and other relevant agencies, including the Prevent programme, to assess and manage identified risks.

The school promotes critical thinking, respectful discussion, digital literacy and media literacy throughout the curriculum to help pupils recognise misinformation, disinformation, extremist narratives and online manipulation.

12. Mental Health

The school recognises that online activity can have both positive and negative impacts on children's mental health and emotional wellbeing. Whilst digital technologies provide valuable opportunities for learning, communication and support, inappropriate or excessive use may contribute to anxiety, low self-esteem, social isolation, exposure to harmful content and other emotional wellbeing concerns.

The school also recognises that concerns relating to a pupil's mental health may be an indicator that they have suffered, or are at risk of suffering, abuse, neglect, exploitation or other forms of harm. Mental health concerns will therefore always be considered within the wider safeguarding context.

Staff will remain vigilant to indicators that online activity may be negatively affecting a pupil's mental health or emotional wellbeing and will respond in accordance with the Child Protection and Safeguarding Policy where safeguarding concerns are identified.

Potential indicators may include, but are not limited to:

- Withdrawal from peers or usual activities.
- Significant changes in mood, behaviour or emotional wellbeing.
- Anxiety or distress linked to online activity.
- Exposure to harmful online content, including content relating to self-harm, suicide or eating disorders.
- Excessive or compulsive use of digital technologies that is affecting education, relationships or wellbeing.
- Online bullying, harassment or exploitation.

Any safeguarding concerns arising from a pupil's mental health or online activity will be reported immediately to the Designated Safeguarding Lead (DSL) and recorded on CPOMS in accordance with the Child Protection and Safeguarding Policy.

Where appropriate, the school will work in partnership with parents, health professionals and external agencies to ensure pupils receive appropriate support.

The school promotes positive mental health, digital wellbeing, balanced use of technology and healthy online behaviours through the curriculum, pastoral support and wider safeguarding arrangements.

13. Online Hoaxes and Harmful Online Challenges

The school recognises that pupils may be exposed to online hoaxes, misinformation, disinformation and harmful online challenges through social media, messaging applications, video-sharing

platforms, gaming platforms and other digital technologies. Such content may place pupils at risk of physical harm, emotional distress or exploitation.

Online hoaxes and harmful challenges can spread rapidly through online platforms and may encourage unsafe, illegal or harmful behaviour. The school will provide pupils with age-appropriate education to help them recognise, question and report harmful online content.

Staff will remain vigilant to emerging online trends and will respond promptly to concerns relating to online hoaxes or harmful online challenges. Any safeguarding concerns will be reported immediately to the Designated Safeguarding Lead (DSL) and recorded on CPOMS in accordance with the Child Protection and Safeguarding Policy.

Where a harmful online challenge or hoax presents an immediate safeguarding risk, the school will take appropriate action to safeguard pupils and, where necessary, work in partnership with parents, the Local Authority, the police or other relevant agencies.

The school will communicate with parents and carers where appropriate to raise awareness of emerging online risks and to support the safe use of technology beyond the school environment.

The curriculum will promote critical thinking, media literacy and digital resilience, enabling pupils to identify unreliable information, question online content and make informed decisions about what they see and share online.

14. Cyber Crime

The school recognises that cyber crime presents a significant risk to individuals, organisations and educational settings. Cyber crime may involve unauthorised access to systems, theft of personal information, malicious software, phishing, ransomware, identity theft, online fraud or other forms of criminal activity involving digital technologies.

The school is committed to promoting cyber security awareness and developing the knowledge and skills of pupils and staff to recognise, prevent and report cyber security risks.

Staff and pupils will receive age-appropriate education on cyber security, including:

- Creating and maintaining strong passwords and passphrases.
- Recognising phishing, smishing and other social engineering techniques.
- Protecting personal and sensitive information.
- Identifying suspicious links, attachments and websites.
- Reporting suspected cyber security incidents promptly.
- Understanding the importance of software updates and secure devices.
- Using multi-factor authentication where available and appropriate.

The school will implement appropriate technical and organisational measures to protect its digital systems and information, including filtering and monitoring, secure authentication, regular software updates, access controls and cyber security procedures.

Any suspected cyber security incident, data breach or malicious online activity affecting the school will be reported immediately to the Headteacher, Finance & Statutory Compliance Manager and ICT Provider. Where a safeguarding concern is identified, the Designated Safeguarding Lead (DSL) will also be informed immediately, and the concern will be recorded on CPOMS where appropriate.

The school will manage cyber security incidents in accordance with the Cyber Security Policy, Data Protection Policy, Child Protection and Safeguarding Policy and relevant incident management procedures.

15. Online Safety Training for Staff

The school is committed to ensuring that all staff receive appropriate online safety training as part of the school's wider safeguarding arrangements. Online safety training forms part of staff induction and is refreshed regularly through safeguarding updates and continuing professional development.

Training will ensure that staff understand:

- Their safeguarding responsibilities in relation to online safety.
- The indicators that a pupil may be at risk of harm online.
- The procedures for reporting online safety concerns in accordance with the Child Protection and Safeguarding Policy.
- The operation and purpose of the school's filtering and monitoring systems.
- Their roles and responsibilities in relation to filtering and monitoring, as outlined in Keeping Children Safe in Education.
- Emerging online risks, including artificial intelligence, online exploitation, cyber crime, harmful online challenges and misinformation.
- The importance of maintaining appropriate professional boundaries when using digital technologies.

The Designated Safeguarding Lead (DSL) will ensure that online safety training is reviewed regularly to reflect changes in legislation, statutory guidance, technology and emerging safeguarding risks.

Where appropriate, additional role-specific training will be provided to staff with particular responsibilities for safeguarding, filtering and monitoring, cyber security or information governance.

The school will maintain appropriate records of safeguarding and online safety training in accordance with its statutory and organisational requirements.

16. Online Safety and the Curriculum

Online safety is embedded throughout the curriculum and forms an integral part of the school's safeguarding and personal development provision. Teaching is age-appropriate, progressive and responsive to emerging technologies, online risks and pupils' developmental needs.

Online safety education is delivered through a range of curriculum areas, including, but not limited to:

- Computing.
- PSHE.
- Relationships Education (RE).

- English.
- History.
- Other curriculum areas where appropriate.

Pupils will be taught the knowledge, skills and behaviours required to use digital technologies safely, responsibly and confidently. Teaching will include, where appropriate:

- Keeping personal information safe online.
- Respectful and responsible online behaviour.
- Recognising online risks and knowing how to seek support.
- Evaluating the accuracy, reliability and credibility of online information.
- Understanding misinformation, disinformation and manipulated content.
- Developing media literacy and critical thinking skills.
- Understanding online relationships, consent and appropriate boundaries.
- Recognising grooming, exploitation and coercive behaviour.
- Cyberbullying prevention and respectful online communication.
- Safe use of social media, gaming platforms and messaging applications.
- Password security, cyber security awareness and protecting personal data.
- Understanding the opportunities, limitations and risks associated with artificial intelligence (AI) and other emerging technologies.
- Understanding age restrictions for online services and digital platforms.
- Developing digital resilience and strategies for managing online challenges safely.

Teaching will reflect current statutory guidance, emerging online risks and the changing digital landscape. Content will be reviewed regularly to ensure it remains relevant, accurate and appropriate to pupils' ages and stages of development.

The school will work in partnership with parents and carers to reinforce key online safety messages and encourage safe, responsible and positive use of technology beyond the school environment.

Where appropriate, online safety education will be supplemented through assemblies, themed events, national awareness campaigns, external speakers and other enrichment opportunities.

17. The Use of Technology in the Classroom

The school recognises that digital technologies enhance teaching, learning and assessment when used safely, responsibly and appropriately. Technology will be used to support high-quality education whilst promoting safeguarding, online safety, inclusion and digital literacy.

Staff will ensure that technology used within the classroom is appropriate to the age, ability and developmental needs of pupils and supports the intended learning outcomes.

When using technology in lessons, staff will:

- Ensure pupils access only approved platforms, applications and online resources.
- Supervise pupils appropriately when using digital technologies.
- Reinforce safe, responsible and respectful online behaviour.
- Consider online safety risks when planning learning activities.
- Promote critical thinking and digital literacy when using online content.

- Protect pupils' personal data and privacy in accordance with the Data Protection Policy.
- Ensure any use of artificial intelligence (AI) supports learning appropriately and is consistent with the school's guidance on AI.

Where online resources, videos or third-party platforms are used, staff will take reasonable steps to ensure content is appropriate, accurate and suitable for the age and maturity of pupils.

The use of technology will always support, rather than replace, effective teaching, professional judgement and meaningful interaction between staff and pupils.

18. Use of Smart Technology

The school recognises that smart technology, including wearable devices, smart watches, voice-enabled devices and other internet-connected technologies, is increasingly common and may present both educational opportunities and safeguarding risks.

Smart technology used within the school will support teaching, learning and operational requirements whilst protecting the privacy, safety and wellbeing of pupils, staff and visitors.

The use of smart technology within the school will be managed in accordance with the Behaviour Policy, Data Protection Policy, Acceptable Use Agreements and this policy.

Where smart technology is used, the school will ensure that:

- Appropriate safeguarding measures are in place.
- Personal data is processed securely and lawfully.
- Devices are used only for authorised educational or operational purposes.
- Audio, video or image recording is not undertaken without appropriate authorisation.
- Devices connected to the school's network meet the school's cyber security requirements.
- Appropriate supervision is maintained when pupils are using smart technology.

Pupils must not use personal smart devices, including smart watches capable of communication, recording or internet access, in a manner that compromises safeguarding, privacy, learning or the effective operation of the school.

Staff will exercise professional judgement when determining whether the use of smart technology is appropriate within the classroom and will consider safeguarding, online safety, privacy, data protection and educational benefit before its use.

Where concerns arise regarding the misuse of smart technology, the school will respond in accordance with the Behaviour Policy, Child Protection and Safeguarding Policy and other relevant school procedures.

19. Educating Parents

The school recognises that parents and carers play a vital role in promoting online safety and supporting children to develop safe, responsible and positive online behaviours. Effective partnership between home and school is essential in safeguarding children in an increasingly digital world.

The school will work proactively with parents and carers to raise awareness of online safety, promote digital resilience and encourage safe use of technology beyond the school environment.

The school will provide parents and carers with appropriate information, guidance and resources to help them:

- Understand current and emerging online safety risks.
- Promote safe, responsible and respectful use of technology at home.
- Recognise indicators that a child may be experiencing online harm, abuse or exploitation.
- Understand age restrictions, privacy settings and parental controls available on digital platforms and devices.
- Support children in developing positive digital habits and digital resilience.
- Encourage open and supportive conversations about online activity.
- Know how to report online safety concerns to the school or other appropriate agencies.

The school will communicate online safety information to parents and carers through a range of appropriate methods, including:

- The school's established communication systems.
- The school website.
- Parent information sessions and workshops.
- Newsletters and safeguarding updates.
- National online safety campaigns and awareness events.
- Information provided by trusted safeguarding organisations, where appropriate.

Where appropriate, the school will provide timely information to parents and carers regarding emerging online risks, trends or incidents that may affect pupils.

The school encourages parents and carers to work in partnership with staff to reinforce online safety messages and promote the safe, responsible and positive use of technology both within and beyond the school environment.

20. Internet Access

The school provides pupils and staff with access to the internet to support teaching, learning, communication and the effective operation of the school. Internet access is recognised as an important educational resource; however, it must be used safely, responsibly and in accordance with the school's safeguarding and acceptable use requirements.

The school will take reasonable and proportionate steps to ensure that internet access is appropriate to the age and needs of pupils and supports a safe online environment.

Access to the internet will be managed through appropriate technical and safeguarding measures, including:

- Appropriate filtering and monitoring systems.
- Secure network management.
- User authentication and access controls.
- Appropriate supervision of pupils when using the internet.
- Age-appropriate access to online resources.

- Regular review of online safety risks and emerging technologies.

Staff will exercise professional judgement when selecting websites, applications and online resources to support teaching and learning. Where appropriate, staff will review online content before it is accessed by pupils to ensure that it is suitable for their age, maturity and educational needs.

Pupils are expected to use the internet safely, responsibly and respectfully, in accordance with the school's Acceptable Use Agreements. Any misuse of internet access will be managed in accordance with the Behaviour Policy, Child Protection and Safeguarding Policy and other relevant school procedures.

Where internet access is provided to visitors or contractors, it will be managed appropriately and in accordance with the school's safeguarding and cyber security arrangements.

21. Filtering and Monitoring Systems

The school recognises that appropriate filtering and monitoring systems are an essential part of its safeguarding arrangements. Filtering and monitoring systems help to reduce the risk of pupils accessing illegal, inappropriate or harmful content, whilst enabling the school to identify, assess and respond appropriately to safeguarding concerns arising from the use of technology.

The school recognises that filtering and monitoring are safeguarding functions and should not be considered solely as technical or ICT responsibilities. Effective arrangements require collaboration between safeguarding, leadership and technical staff.

The school will implement filtering and monitoring arrangements that are appropriate to the age and needs of pupils, the curriculum, the school's safeguarding risk profile and the requirements of the Department for Education's Filtering and Monitoring Standards.

Filtering and monitoring arrangements will be reviewed regularly to ensure they remain effective, proportionate and responsive to emerging technologies, online risks and changes in statutory guidance.

21.1. Filtering

The school will implement appropriate filtering systems designed to reduce the likelihood of users accessing illegal, inappropriate or harmful online content whilst supporting legitimate teaching, learning and research activities.

The school's filtering arrangements will seek to:

- Block access to illegal online content.
- Restrict access to inappropriate or harmful material.
- Apply age-appropriate filtering for pupils.
- Support teaching and learning by allowing access to appropriate educational resources.
- Be reviewed where legitimate educational requirements necessitate access to otherwise restricted content.

21.2. Monitoring

The school will implement appropriate monitoring systems to help identify safeguarding concerns and inappropriate use of technology, whilst recognising that no monitoring system can identify every potential risk.

Monitoring arrangements may assist in identifying:

- Attempts to access harmful or inappropriate content.
- Cyberbullying or abusive online behaviour.
- Indicators of grooming, exploitation, radicalisation or child-on-child abuse.
- Attempts to bypass filtering systems or security controls.
- Unusual or suspicious online activity.
- Potential cyber security incidents.
- Other safeguarding concerns requiring further assessment.

Where monitoring systems identify a potential safeguarding concern, the matter will be assessed by the Designated Safeguarding Lead (DSL) and managed in accordance with the Child Protection and Safeguarding Policy. Safeguarding concerns will be recorded on CPOMS where appropriate.

21.3. Roles and Responsibilities

The Headteacher, Designated Safeguarding Lead (DSL), SLT and ICT Provider will work collaboratively to ensure that filtering and monitoring arrangements remain effective, proportionate and compliant with statutory guidance.

The:

- Headteacher has overall responsibility for ensuring appropriate filtering and monitoring arrangements are implemented within the school.
- Designated Safeguarding Lead (DSL) is responsible for reviewing safeguarding concerns identified through monitoring systems and ensuring appropriate safeguarding action is taken.
- SLT is responsible for supporting compliance with the Department for Education's Filtering and Monitoring Standards, coordinating the periodic review of filtering and monitoring arrangements and maintaining appropriate records of those reviews.
- ICT Provider is responsible for implementing, maintaining and supporting the school's filtering and monitoring systems, applying appropriate technical controls and reporting any technical concerns or vulnerabilities promptly.

21.4. Review and Continuous Improvement

Filtering and monitoring arrangements will be formally reviewed at least annually and whenever there are significant changes to technology, safeguarding risks or statutory guidance.

The review will consider, where appropriate:

- The school's safeguarding risk profile.
- The age and needs of pupils.
- The curriculum and educational requirements.
- The effectiveness of current filtering and monitoring arrangements.

- Emerging online risks, including artificial intelligence and AI-generated content.
- Cyber security risks and vulnerabilities.
- Safeguarding incidents and trends.
- Feedback from safeguarding staff, the ICT Provider and other relevant stakeholders.

Where school-managed devices are used off-site, the school will seek to ensure that appropriate filtering and monitoring arrangements continue to operate wherever this is technically possible and proportionate.

The outcomes of filtering and monitoring reviews will be documented and used to inform safeguarding practice, staff training, risk assessments, procurement decisions and future improvements.

21.5. Staff Awareness

All staff will receive appropriate information regarding the purpose and operation of the school's filtering and monitoring systems as part of safeguarding induction, training and regular safeguarding updates. Staff are expected to understand their role in identifying, reporting and responding to concerns identified through filtering and monitoring arrangements.

21.6. Visitors and Contractors

Visitors and contractors using school devices or networks will be subject to the school's filtering and monitoring arrangements where appropriate.

The school recognises that filtering and monitoring systems reduce, but cannot eliminate, online risk. Effective safeguarding therefore relies upon a combination of appropriate technical controls, staff vigilance, pupil education, professional judgement and effective safeguarding procedures.

The school will continue to review emerging technologies, including generative artificial intelligence (AI), to ensure that its filtering and monitoring arrangements remain appropriate, effective and responsive to new and evolving online risks.

22. Network Security

The school is committed to maintaining a secure and resilient digital environment that supports teaching, learning and the effective operation of the school whilst protecting pupils, staff, visitors and school information from cyber security threats.

Appropriate technical and organisational measures will be implemented to reduce the risk of unauthorised access, cyber attacks, data loss and other security incidents affecting the school's network, systems and devices.

The school will work in partnership with its ICT Provider to ensure that appropriate network security arrangements are maintained, including, where appropriate:

- Secure network infrastructure.
- Appropriate user authentication and access controls.
- Strong password and passphrase requirements.
- Multi-factor authentication (MFA), where available and appropriate.

- Appropriate filtering and monitoring systems.
- Anti-virus and anti-malware protection.
- Firewalls and network security controls.
- Regular software updates and security patching.
- Secure backup and recovery arrangements.
- Appropriate management of user accounts and permissions.
- Secure remote access arrangements, where applicable.
- Appropriate cyber security monitoring and incident detection.

Access to the school's network will be restricted to authorised users and devices. User access permissions will be allocated according to business need and reviewed periodically to ensure they remain appropriate.

The school recognises that cyber security is a shared responsibility. All staff are expected to follow the school's cyber security procedures, use school systems responsibly and report any suspected cyber security incidents, vulnerabilities or suspicious activity immediately.

Where a cyber security incident has the potential to impact safeguarding, personal data or the continuity of school operations, the Headteacher, SLT, Designated Safeguarding Lead (DSL) and ICT Provider will work collaboratively to manage the incident in accordance with the Cyber Security Policy, Data Protection Policy and Child Protection and Safeguarding Policy, where appropriate.

The school will regularly review its network security arrangements to ensure they remain effective, proportionate and responsive to emerging cyber security threats, technological developments and current best practice.

23. Emails

The school recognises that email is an important communication tool and must be used safely, responsibly and professionally. All users are expected to use email in a manner that protects safeguarding, confidentiality, information security and the reputation of the school.

School email accounts will be used for school business and professional communication. Personal use must be limited and must not interfere with an individual's professional responsibilities or compromise the security or reputation of the school.

Users must:

- Use only authorised school email accounts for school business.
- Take reasonable steps to verify the identity of recipients before sending sensitive or confidential information.
- Exercise caution when opening emails, attachments or links from unknown or unexpected sources.
- Report suspected phishing emails, malicious attachments or other suspicious communications immediately to the ICT Provider.
- Ensure personal data is processed in accordance with the Data Protection Policy and UK GDPR.
- Maintain appropriate professional standards when communicating by email.

- Protect login credentials and not share passwords with others.

Users must not:

- Send, forward or store offensive, inappropriate or discriminatory material.
- Use school email accounts for unauthorised commercial, political or personal purposes.
- Circumvent the school's security controls.
- Share confidential information with unauthorised individuals.

The school will implement appropriate technical measures to help protect email systems from cyber security threats, including spam, phishing, malware and other malicious activity.

Where an email-related incident has safeguarding implications, the matter will be reported immediately to the Designated Safeguarding Lead (DSL) and managed in accordance with the Child Protection and Safeguarding Policy. Where personal data is involved, the incident will also be managed in accordance with the Data Protection Policy and the school's data breach procedures.

24. Generative AI

The school recognises that generative artificial intelligence (AI) is an increasingly common feature of education, communication and everyday life. When used appropriately, AI has the potential to enhance teaching, learning, accessibility and administrative efficiency. However, AI also presents safeguarding, educational, ethical, privacy and information security risks that require careful management.

The use of generative AI within the school will always support, and never replace, professional judgement, effective safeguarding practices and high-quality teaching.

Staff and pupils may only use generative AI tools that have been approved or authorised by the school where appropriate.

Where generative AI is used, staff will ensure that:

- Its use is appropriate to the age and needs of pupils.
- Appropriate safeguarding measures are maintained.
- Personal, confidential or sensitive information is not entered into public AI platforms.
- AI-generated content is reviewed for accuracy, bias, suitability and educational value before being used.
- Copyright, intellectual property and licensing requirements are respected.
- AI is used in accordance with the Data Protection Policy, Acceptable Use Agreements and other relevant school policies.

Pupils will be taught to understand:

- What generative AI is and how it works.
- The opportunities and limitations of AI technologies.
- That AI-generated content may be inaccurate, biased or misleading.
- How to evaluate AI-generated information critically.
- The importance of protecting personal information when using AI tools.
- The ethical and responsible use of AI.

The school recognises that AI technologies may contribute to safeguarding risks, including:

- AI-generated misinformation and disinformation.
- Deepfake images, audio and video.
- AI-assisted cyberbullying.
- AI-facilitated grooming or exploitation.
- Academic dishonesty.
- Privacy and data protection risks.

Where AI is used to support school operations, appropriate consideration will be given to safeguarding, privacy, cyber security, copyright, equality and data protection requirements before implementation.

The school will regularly review developments in artificial intelligence and update its policies, procedures, curriculum and staff training to reflect emerging technologies, safeguarding risks and statutory guidance.

25. Social Networking

The school recognises that social networking platforms and other online communities present both educational opportunities and safeguarding risks.

The school will educate pupils about the safe, responsible and respectful use of social networking platforms through the curriculum and wider online safety education programme, including the importance of protecting personal information, maintaining appropriate privacy settings, recognising online risks and reporting concerns to a trusted adult.

Staff are expected to maintain appropriate professional boundaries when using social networking platforms and must not communicate with pupils through personal social media accounts or other unauthorised online platforms. Staff must comply with the Staff Code of Conduct, Social Media Policy and Acceptable Use Agreements.

Where the use of social networking platforms gives rise to safeguarding concerns or impacts upon the safety, wellbeing or education of pupils, the matter will be managed in accordance with the Child Protection and Safeguarding Policy and Behaviour Policy, where appropriate.

26. The School Website

The school website supports communication with pupils, parents, carers and the wider community. The school is committed to ensuring that all content published on the website is appropriate, accurate, accessible and compliant with relevant legislation.

The school will take reasonable steps to ensure that information published on the website does not compromise the safeguarding, privacy or security of pupils, staff or visitors.

Any photographs, videos or other media featuring pupils will only be published where appropriate consent has been obtained and in accordance with the school's Data Protection Policy, Photography Policy and other relevant procedures.

Website content will be reviewed periodically to ensure that it remains accurate, appropriate and up to date.

Further information regarding the management of the school website is contained within the Trust's Website Policy.

27. Use of Devices

The school recognises that digital devices play an important role in teaching, learning and the effective operation of the school. The use of school-owned and personal devices must support safeguarding, learning, information security and the wellbeing of the school community.

School devices will be provided and managed to support educational and operational purposes. Users are expected to use all devices safely, responsibly and in accordance with this policy, the Acceptable Use Agreements and other relevant school policies.

Where personal devices are permitted, their use must not compromise safeguarding, learning, privacy, data protection or the security of the school's network and systems.

Users must:

- Use devices responsibly and only for authorised purposes.
- Protect devices from unauthorised access or misuse.
- Take reasonable care of school-owned devices.
- Report lost, stolen or damaged devices without delay.
- Report any safeguarding, cyber security or technical concerns immediately.

The school reserves the right to restrict or withdraw access to devices where they are used inappropriately or where their use presents a safeguarding, security or operational risk.

Further guidance regarding the acceptable use and management of devices is contained within the school's Acceptable Use Agreements, Behaviour Policy, Mobile Phone Policy (where applicable) and Cyber Security Policy.

28. Remote Learning

The school recognises that remote learning may be required in certain circumstances to support continuity of education. Where remote learning takes place, the school will ensure that appropriate safeguarding, online safety and data protection arrangements remain in place.

Remote learning will be delivered using approved platforms and technologies authorised by the school. Staff and pupils are expected to use these platforms safely, responsibly and in accordance with the school's Acceptable Use Agreements and relevant school policies.

When delivering remote learning, staff will:

- Maintain appropriate professional boundaries.
- Use only approved communication platforms and school accounts.
- Protect the privacy and personal data of pupils and staff.

- Report safeguarding concerns immediately in accordance with the Child Protection and Safeguarding Policy.
- Promote safe and responsible online behaviour throughout remote learning activities.

Pupils are expected to participate in remote learning safely, respectfully and responsibly, following the school's expectations for behaviour and online conduct.

Parents and carers are encouraged to support pupils in accessing remote learning safely and to report any safeguarding or online safety concerns to the school promptly.

Further guidance regarding the delivery of remote education is contained within the school's Remote Education Policy and other relevant procedures.

29. Protecting Personal Information

The school is committed to protecting the personal information of pupils, staff, parents, carers and visitors when using digital technologies.

All users are expected to handle personal information securely and in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the school's Data Protection Policy and other relevant procedures.

Users must take reasonable steps to:

- Protect personal and confidential information from unauthorised access or disclosure.
- Use only approved systems and platforms for processing school information.
- Verify recipients before sharing personal information electronically.
- Report actual or suspected data breaches immediately in accordance with the school's Data Protection Policy.

The school will promote good information governance practices to ensure that personal information remains secure and is processed lawfully, fairly and transparently.

30. Educational Apps and Third-Party Platforms

The school recognises that educational applications, online platforms and third-party digital services can enhance teaching, learning and communication. However, their use must be carefully managed to ensure safeguarding, data protection, cyber security and educational suitability.

Only applications, websites and digital platforms that have been approved by the school may be used for teaching, learning or communication with pupils.

Before introducing a new digital platform or application, the school will consider, where appropriate:

- Safeguarding and online safety implications.
- Data protection and UK GDPR compliance.
- Age appropriateness and educational suitability.
- Cyber security arrangements.
- Accessibility and inclusion.

- The reputation and reliability of the provider.

Staff are responsible for ensuring that digital platforms are used safely, appropriately and in accordance with this policy, the Data Protection Policy, Acceptable Use Agreements and other relevant school procedures.

The school will review approved platforms periodically to ensure they remain suitable, secure and compliant with current legislation, statutory guidance and educational best practice.