

South East Essex Academy Trust



On-line Safety Policy 2026

Title	On-line Safety Policy 2026
Author	Caroline Thornton
Owner	SEEAT
Status	Pending
Ratified Date	24 th September 2026
Ratified by	Approved by the Education Committee adopted by the Local Governing Body (LGB)
Review Cycle	Annual
Review Date	September 2027

Part 1 - (School Name) On-line Safety Information and Key Contacts

Governor with responsibility for on-line safety.	Nuala Harber
Name External IT provision provides your schools filtering and monitoring systems?	SEEAT IT Support
Name of filtering system in use	Smoothwall
The Designated Safeguarding Lead with responsibility for filtering and monitoring	Mrs T.Dennis
Other named staff supporting the Designated Safeguarding Lead with On-line Safety	Mr N. Dubouchet Mrs L. Hargreaves Mr J.Holmwood Miss S. Emmerton
Name of IT Lead/ Network Manager	Mr D. Sanders
Mobile Phones	https://www.princeavenue.co.uk/docs/policies/SEEAT_Mobile_Phone_Policy_PAAN_.pdf
Governor with responsibility for Safeguarding (if different from above)	As above

Contents

1	School Information and Key Contacts
2	Online Policy Statement
2.1	Policy Aims
2.2	Legislation and Guidance
3	Roles and Responsibilities
3.1	The Trust Board
3.2	The Local Governing Body
3.3	All Governors
3.4	Head teachers/ Executive Heads and Heads of School
3.5	Designated Safeguarding Lead
3.6	School IT Leads and Network Managers
3.7	SEEAT ICT Manager
3.8	All Staff
3.9	Subject, Curriculum and Year Group Managers
3.10	Parents and carers
3.11	Pupils
3.12	Visitors, Volunteers & Members of the School Community
4	Educating Pupils Online
5	Educating Parents about Online Safety

6	Cyberbullying
7	Acceptable use of the Internet in School
8	Staff using Work Owned Devices outside of School
9 9.1 9.2	Guest Devices – Bring Your Own Device (BYOD) Pupils BYOD Staff and Visitors
10	Monitoring the use of Mobile Devices
11 11.1	Pupils using Mobile Phones in School Staff Mobile Phone Use
12	Responding to Incidents of Misuse
13	Examining Electronic Devices
14 14.1 14.2	Social media and Online Communication Platforms Expected Conduct on social media Inappropriate and unprofessional use of social media
15	Training
16	Technical Security
17 17.1 17.2	Artificial Intelligence (AI) AI Governance Staff use of AI

17.3	Pupil use of AI
17.4	AI Safeguarding Risks
17.5	Filtering and Monitoring of AI
18	Filtering and Monitoring
18.1	Filtering
18.2	Illegal On-line Content
18.3	Inappropriate On-line Content
18.4	Filtering System Features
18.5	Filter Testing
18.6	Monitoring
Appendices 1	Links with other policies
Appendices 2	Appropriate use Agreements
Appendices 3	Audit and Testing Tools

2. On-line Safety Policy Statement

This On-line Safety Policy outlines the commitment of SEEAT (South East Essex Academy Trust) to safeguard members of our school community online in accordance with statutory guidance and best practice.

This Online Safety Policy applies to all members of the school community including staff, learners, governors, volunteers, parents and carers, visitors, and community users, who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Our schools will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

2.1 Policy Aims

SEEAT aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which includes any mobile device, including phones)
- Set out expectations for all school community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible, and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online

- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
 - for the protection and benefit of the children and young people in their care, and
 - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
 - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

The 4 key categories of risk

The DfE (Department for Education) *Keeping Children Safe in Education* guidance suggests that:

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation, conspiracy theories, manipulated media, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending, and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2.2 Legislation and guidance

This policy is based on the Department for Education's (DfE) [Filtering and Monitoring Standards for Schools](#) and [Keeping Children Safe in Education 2026](#)

It also details advice for schools on:

- [Teaching online safety in schools](#)

- [Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and Sex Education 2026](#)
- [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#), [Equality Act 2010](#).

In addition, it outlines the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

This policy complies with our funding agreement and articles of association

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and Responsibilities

SEEAT is a family of schools and all members of our community have a duty to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere. We use technology for teaching and learning and to prepare pupils for life after school. Any concerns or inappropriate behaviour are reported, to protect pupils, staff, families and the reputation of the school.

While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school. Everyone is expected to:

- Understand and implement this policy consistently
- Agree and adhere to the terms of the acceptable use agreement relevant to their role
- Ensure pupils adhere to the acceptable use agreement relevant to them
- Know who the DSL is and how to report any incidents or system failures

3.1 The Trust Board

The SEEAT Trust Board ensure that this policy is reviewed annually and meets statutory requirements and best practice. It will ensure that:

- Training is in place that meets statutory requirements and best practice
- Ensure their school provides an appropriate level of filtering and monitoring which safeguards young people from risky online content and contact
- Ensure that there is sufficient capability and capacity in those responsible for, and those managing, the filtering system (including any external support provider)

- Receive and act upon online safety reports from senior leaders and the LGB

3.2 The Local Governing Body (LGB)

The SEEAT Trust Board has delegated to the LGB (in each SEEAT school) the responsibility for monitoring this policy and holding the Headteacher/Executive Headteacher/Head of School to account for its implementation. As part of their monitoring, the governor responsible for safeguarding will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

Governors are responsible for approving the Online Safety Policy and reviewing its effectiveness. This review will be carried out by the named member of the governing body with responsibility for on-line safety and will include:

- Regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- Regularly receiving an anonymised overview of online safety incidents and actions taken to remediate concerns
- Support and critically challenge the school in implementing effective online safety policy, procedure, and practice
- Ensure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring
- Ensuring appropriate filters and appropriate monitoring systems are in place, but being careful that ‘overblocking’ does not lead to unreasonable restrictions on pupil’s learning
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually in line with the [DfE Filtering and Monitoring Standards](#)
- Reporting to relevant governors group/meeting
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the [DfE Cyber-Security Standards](#)

3.3 All governors will:

- Ensure that they have read and understand this policy
- Have an awareness of online threats, risks and trends in technology use and internet use
- Ensure that online safety is a running and interrelated theme and part of the implementation of the MAT/school safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a ‘one size fits all’ approach may not be appropriate for all children in

all situations, and a more personalised or contextualised approach may often be more suitable

- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

3.4 The Headteacher/Executive Headteacher/Head of School

The headteacher/Executive Headteacher/Head of School is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

They have a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education. They will:

- Ensure that at least one other member of the senior leadership team is aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff
- Ensure that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues
- Receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead
- Work in partnership with the named governor, the designated safeguarding lead (DSL)

The Headteacher/Executive Headteacher/Head of School and/ or members of the schools leadership team are responsible for monitoring and approving requests for specific online sites to be unblocked at the request of school staff. Any request made to the headteacher or leadership team to unblock a site will:

- Consider the relevance of the request in relation to the curriculum
- Ensure that the site/ materials are appropriate for use in the classroom and for the purposes requested
- Consider whether a restriction should be lifted permanently, or for a time limited period
- Record the decision and rationale for agreeing a block should be lifted

Note: Whilst ensuring appropriate filters and monitoring systems are in place, they must be cautious about 'overblocking' which may lead to unreasonable restrictions on learning, including being taught about online safety.

3.5 The Designated Safeguarding Lead (DSL)

The designated safeguarding lead is responsible for safeguarding and child protection, including online safety and understanding the filtering, and monitoring systems and processes. This should be explicit in the role holder's job description.

The DSL is required to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe while they are at school.

The responsibility for online safety is held by the DSL and cannot be delegated, but the school may choose to designate another appropriately qualified, relevant person to support the DSL in carrying out these responsibilities depending on the structure of the individual school. The designated staff member must liaise closely, on a day-to-day basis, with the DSL.

The DSL must be able to recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example from bullying, grooming and radicalisation. In partnership with the SENDCo, they will ensure that online safety education, support and safeguarding responses are adapted to meet the needs of individual pupils.

Some pupils may be at greater risk online, including children with SEND, children with social, emotional or mental health needs, looked-after children, previously looked-after children and children who are vulnerable to exploitation. Schools will ensure that online safety education and safeguarding responses are adapted where required to reflect individual vulnerabilities, needs and risks.

The Trust recognises that online harms frequently form part of wider contextual safeguarding concerns. Online activity may facilitate bullying, exploitation, peer-on-peer abuse, criminal exploitation, sexual exploitation, radicalisation, harmful sexual behaviour and abuse beyond the home environment. Online concerns will be considered alongside all available safeguarding information to ensure a full and effective assessment of risk, vulnerability and need. Schools will respond to online safety concerns in accordance with the Child Protection and Safeguarding Policy and will work with pupils, families and external agencies where appropriate.

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, within their role to include:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Be responsible for receiving reports of online safety incidents and investigating them as appropriate
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy and the Safeguarding and Child Protection Policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT / Network manager to make sure the appropriate systems and processes are in place and working effectively
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Providing safeguarding and child protection training, including online safety (at least annually)
- Providing updates throughout out the year on new technologies, trends, local context and other newly identified risks which may impact on student safety on-line
- Liaising with other agencies and/or external services as required
- Providing regular reports on online safety in school to the headteacher, Trust and the governing board
- Liaise with senior leaders and the curriculum leader to ensure the online safety curriculum is planned, mapped, embedded, and evaluated
- ensure that all staff are aware of the procedures to be followed if there is an online safety incident
- Provide, or identify sources of training and advice for staff, governors, parents & guardians, and learners
- Liaise with school, local authority, SEEAT central team, external providers, technical staff, pastoral teams, and support staff (as relevant)
- Receive regularly updated training to allow them to understand how digital technologies are developing and being used (particularly by learners) regarding the areas defined In Keeping Children Safe in Education:
 - content
 - contact
 - conduct
 - Commerce

3.6 School IT Leads and Network Managers

The day-to-day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSLs should work closely with school IT Leads/ Network Managers and external providers to ensure an adequate level of security.

The IT Lead/ Network Manager (School specific) has technical responsibility for:

- Keeping up to date with the school's online safety policy and technical information to effectively carry out their online safety role and to inform and update others as relevant
- Maintaining school systems
- Maintaining filtering and monitoring systems
- Being alert to risk and keeping up abreast of evolving technologies and trends
- Providing filtering and monitoring reports to the DSL and headteacher
- Ensuring the SEEAT Online Safety Policy to be able to carry out their work effectively and in line with said policy
- Running filtering test using [Filtering Test](#). Test should be completed half termly as minimum, and in response to breaches and security concerns
- Working with the Headteacher to ensure the school website meets statutory DfE requirements
- Reporting online-safety related issues that come to their attention in line with school policy
- Working closely with the designated safeguarding lead, senior leaders SEEAT central IT team to ensure that school systems and networks reflect school policy

3.7 The SEEAT ICT Manager (and team, as deployed by them) is responsible for:

- Ensuring an appropriate level of security protection procedures, such as filtering and monitoring systems on trust wide devices and networks, which are reviewed and updated at least annually to assess their effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact including terrorist and extremist material online while at school
- Ensuring the trusts technical infrastructure is secure and is not open to misuse or malicious attack
- Ensuring that schools meet (as a minimum) the required online safety technical requirements as identified by the [DfE Meeting Digital and Technology Standards in Schools & Colleges](#) and guidance from local authority / MAT (Multi Academy Trust) or other relevant body
- Ensuring clear, safe, and managed control of user access to networks and devices
- Keeping up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

- Ensuring the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported for investigation and action
- Ensuring the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- Ensuring school digital systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a security check and monitoring SEEAT wide systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Completing actions following concerns or checks to systems
- Ensuring the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc

The SEEAT ICT Manager should work with the trust leaders, senior leadership team and DSL's to:

- Procure systems
- Identify risk
- Work in partnership to carry out reviews and checks
- Ensure that external technology/ systems providers implement all the online safety measures that school obligations and responsibilities require

3.8 All Staff

All staff, including contractors and agency staff, students and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use (see appendices 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing
- Following the correct the procedures of the school if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this and other related policies

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Notify the DSL if you believe policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- Prepare and check all online source and resources before using within the classroom
- Encourage pupils to follow their acceptable use policy, and observe the behaviour policy where they do not
- Notify the DSL of the latest trends, games and apps which may present a safety risk to pupils
- Take a zero-tolerance approach to bullying and sexual harassment
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL know
- Have a healthy curiosity for online safety issues
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff. More guidance on this point can be found in this [Online Reputation](#) guidance for schools.

3.9 Subject, Curriculum and Year Group Leaders

Subject, Curriculum and Year Group Leaders work with the DSL and school leaders to develop a planned and coordinated online safety approach, which threads through the curriculum and other aspects of school life. This will vary for school-to-school, and may include:

- computing lessons
- Clubs and activities
- Personal Development programme
- Tutor programme
- PHSE and RSE (Relationship and Sex Educations) (Relationships and Sex Education) programmes
- a mapped cross-curricular programme
- Assemblies
- pastoral programmes and interventions
- workshops and targeted groups
- Participation in relevant local and national initiatives and opportunities, for example, [Safer Internet Day](#) and [Anti-bullying week](#).

Topics such as consent, mental health & wellbeing, healthy relationships and staying safe online are embedded in RSE/PSHE curriculum and complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully, and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Mental Health and Wellbeing

Schools recognise that online experiences can have a significant impact on emotional wellbeing and mental health. Exposure to bullying, social pressures, harmful content, body image pressures, self-harm content, suicide-related content, misinformation and online abuse can adversely affect wellbeing. Schools will work with pupils, families and relevant agencies to support children affected by online harms.

3.10 Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use online technologies and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images and cloud services for example, as determined by the individual school
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers are asked to support the school by:

- reinforcing the online safety messages provided to learners in school
- checking their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet
- Encouraging the safe and responsible use of their children's personal devices in the school (where this is allowed)
- notifying a member of staff or the headteacher of any concerns or queries regarding this policy on online safety

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#)
- Hot topics – [Childnet International](#)
- Parent resource sheet – [Childnet International](#)

3.11 Pupils

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy, including on personal devices where they are allowed
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

3.12 Visitors, Volunteers, and members of the Community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when they first visit the school. They will also be made aware of how to raise a concern. All visitors are expected to:

- read and follow the Online Safety Policy
- agree to the terms on acceptable use if asked to do so (appendix 2)
- report any concerns regarding online safety or abuse to the DSL
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible, and professional behaviour in their own use of technology

The school encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum, throughout their education.

All schools must teach:

- [Relationships education and health education](#) in primary schools
- [Relationships and sex education and health education](#) in secondary schools

In Key Stage 1, pupils will be 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

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous

- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

Secondary schools

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

In **Key Stage 4**, pupils will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online

- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND. Pupils of all ages will be taught about online safety as part of the curriculum.

Teaching will include AI literacy, critical evaluation of AI generated content, misinformation and digital resilience.

5. Educating parents about online safety

Schools will raise parents' awareness of internet safety in letters and other communications home, and in information via our website or social media platforms.

This policy will be shared with parents. Online safety may also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with their school's Headteacher/Executive Headteacher/Head of School and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher/Executive Headteacher/Head of School.

The school will let parents/carers know how the school filters and monitors online activity.

6. Cyber-bullying

Definition: Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups.

Teaching staff are encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, Computing lessons, assemblies and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also provides information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy.

Where illegal, inappropriate, or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only or for fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendix 2.

8. Staff using work devices outside of school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers, and special characters (e.g. asterisk or currency symbol)
- Ensuring that files are stored on the school's network. This means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period
- Not sharing the device among family or friends
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way, which would violate the school's terms of acceptable use, as set out in appendix 2. Work devices must be used solely for work activities. Work devices can only be used by the employee and not by family members.

Staff must store equipment safely, e.g. not leaving the device in a vehicle unattended.

Staff must not download their own apps or software onto a school device. If staff have any concerns over the security of their device, they must seek advice from their Headteacher or IT Lead.

9. Guest Devices - Bring Your Own Device (BYOD)

9.1 Pupils BYOD

SEEA does not have a trust wide policy about students bringing their own devices to school. Therefore, each school has their own policy on guest devices/ BYOD. Please refer to part 1, titled 'School Information and Key Contacts' of this document to access the link to the school BYOD Policy.

9.2 Staff and Visitors

We recognise that mobile technology offers valuable benefits to staff, students and visitors from a teaching and learning perspective.

Our Trust embraces this technology but requires that it be used in an acceptable and responsible way.

Guest devices include laptops, tablets, smart phones, wearable technology (including smart / apple watches) and any other device considered portable and/or with the ability to connect to Wi-Fi and the Internet which is not school owned or on the school asset list, including staff personal devices.

Access to the network is at the discretion of the school, and the school may withdraw access from anyone it considers is using the network inappropriately.

Schools should not compel school staff to bring their own devices to access school systems, but **if** staff are allowed, and choose to bring their own devices, the following points must be adhered to:

- Guest devices (any device which is not school owned or on the school asset list) should only be connected to the schools network
- This guidance is designed to support the use of guest devices (any device which is not school owned or on the school's asset list) in schools in a way that extends and enhances teaching and learning. It also aims to protect children from harm, minimise risk to the school networks and explain what constitutes acceptable use and misuse

10. Monitoring the use of mobile devices

The Trust/school uses technology that filters and monitors the use of personal devices which are connected to the school network. The use of such technology is for the purpose of ensuring the security of its IT systems and school information.

Any search for content which is illegal or on the school block list will be identified on the daily reports received by the school.

Alerts are received in two ways. Live alerts will immediately notify the head teacher of searches for sites with illegal content, or pose a risk, or perceived risk to pupil or adult safety is identified.

The SafeSearch function is automatically enforced for all major search engines.

Note: Guest devices are subject to the same scrutiny as school owned devices.

11. Pupils using mobile phones in school

SEEAT does not have a trust wide policy about students bringing mobile phones to school. This is because of the wide age range of the pupils in our schools, and because of the vast difference in travel times and arrangements for some learners.

Therefore, each school has their own policy on mobile phone use. Please refer to part 1, titled **'School Information and Key Contacts'** of this document to access the link to the school Mobile Phone Policy.

11.1 Staff Mobile Phone Use

At SEEAT we recognise that mobile phones play an important part in our lives and when used as they are intended, can bring substantial benefits.

We also acknowledge that there is a risk that they can be used for the taking, storing, and using of images inappropriately.

They also have the potential to distract staff from their work with students.

Staff members (including volunteers and students on placement) may bring mobile phones onto the school site on the understanding that the device:

- Is used only in the staffroom, outside of the school gate, or in office spaces when no students are present

- Only used during break times and at either end of the school day
- When off-site, designated members of the group will have a mobile phone available for emergency contact with the school, with each other or with the emergency services. In this context phones will not be used to make or receive personal calls
- Personal mobile phones must not be used to take photos of students except in very exceptional circumstances when permission from a senior leader must be sought and granted in advance and the image erased as soon as possible in the presence of a work colleague
- Visitors may bring mobile phones on to the school site but are asked to switch them off and place them out-of-sight until they leave exiting the school gates/reception. This is done as part of the meet-and-greet process in a way that makes clear our safeguarding priorities.

Infringements to this guidance will be addressed through the SEEAT Code of Conduct Policy

12. Responding to incidents of misuse

School's will take all reasonable precautions to ensure online safety for all users but recognises that incidents may occur inside and outside of the school, and that those which happen outside of school will continue to impact on pupils when they come into school.

All members of the Trust are encouraged to report issues swiftly to allow the DSL, senior leaders and the IT Manager to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the designated safeguarding lead. If there is an immediate risk to safety the concern must be reported immediately.

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Safeguarding and Child Protection, Behaviour and the internet acceptable use agreement. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. We will inform parents/carers of online-safety incidents involving their children and notify them of referrals to external partners such as the police and social care where necessary.

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 disciplinary procedures/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.

Pupils	attending	Alternative	Provision
Where pupils access alternative provision or other off-site educational placements, schools remain responsible for ensuring appropriate safeguarding arrangements are in place. This includes seeking assurance that online safety expectations, filtering and monitoring arrangements, reporting procedures and safeguarding practices are appropriate to the age, needs and risks of the pupil and the nature of the placement.			

The school will actively seek support from other agencies as needed (i.e. the local authority, CEOP, Prevent Officer and the Police).

Support and Early Help

Where online behaviours indicate emerging safeguarding, welfare or wellbeing concerns, schools will adopt a support-first approach and consider whether early help, pastoral support, safeguarding intervention or specialist services may be required. Responses will be proportionate to the needs and risks identified and will be developed in partnership with pupils, families and relevant agencies where appropriate.

General concerns will be investigated and managed in the same way as any other safeguarding concern. The school will ensure:

- There are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policy
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is possible once they are received
- the Designated Safeguarding Lead, or other delegated responsible staff have appropriate skills and training to deal with online safety risks.
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm ([see flowchart and user actions chart in the appendix](#)), the incident will be escalated. Examples
 - o Non-consensual images
 - o Self-generated images
 - o Terrorism/extremism
 - o Hate crime/ Abuse
 - o Fraud and extortion
 - o Harassment/stalking

- o Child Sexual Abuse Material (CSAM)
- o Child Sexual Exploitation Grooming
- o Extreme Pornography
- o Sale of illegal materials/substances
- o Cyber or hacking [offences under the Computer Misuse Act](#)
- o Copyright theft or piracy

13. Examining Electronic Devices

The Headteacher/Executive Headteacher/Head of School, and any member of staff authorised to do so by them, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- o Assess how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher/Executive Headteacher/Head of School/ DSL/Senior Leader
- o Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- o Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / Headteacher/Executive Headteacher/Head of School or other member of the senior leadership team to decide on a suitable response.

If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response. When deciding if

there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Note: Any searching of pupils will be carried out in-line with the afore-mentioned guidance.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school's Complaints Procedure.

14. Social media and online communication platforms

Social media and online communication platforms include, but are not limited to, social networking sites, messaging and chat applications, online forums, blogs, microblogs, podcasts, gaming communication platforms, livestreaming services, video and content sharing sites, collaborative online spaces, open-access encyclopedia's, artificial intelligence (AI) chat and communication tools, and any other digital platform that enables users to create, share, view or exchange content, messages or information. Examples may include platforms such as Instagram, Facebook, Snapchat, TikTok, WhatsApp, Discord, X (formerly Twitter), YouTube and similar services, recognising that platforms and technologies continue to evolve.

All members of staff should be aware that information shared through social media and online communication platforms, including content shared within private groups, closed networks or personal accounts, may still be subject to data protection legislation, copyright law, Freedom of

Information requirements, safeguarding responsibilities, professional standards and other relevant legislation and guidance.

Staff should understand that many social media and online communication platforms have minimum age requirements and that pupils should not be encouraged to create accounts that do not comply with a platform's terms of service. Any communication received by staff from pupils through personal social media accounts or online communication platforms must be reported to the Designated Safeguarding Lead (DSL). Likewise, any inappropriate, concerning or potentially harmful online communication involving a child, whether occurring on social media, messaging services, gaming platforms or other online environments, must be reported immediately in accordance with safeguarding procedures.

14.1 Expected conduct on social media

It is important and expected that staff follow the following guidance:

- Staff are advised to avoid posts or comments that refer to specific, individual matters related to the Trust or school and members of its community on any social media accounts, unless it is an official post or retweeting school information
- Staff should not comment on the Trust or their school, or any other Trust or Academy official social media page from their personal account
- Staff are also advised to consider the reputation of the Trust in any posts or comments related to the Trust on any social media accounts
- Staff should not accept any current student of any age or any ex-pupil of the school under the age of 18 as a friend, follower, subscriber or similar on any personal social media account, except for relatives
- Never 'friend' a student at any school in the trust where they are working onto their social networking site
- Be conscious at all times of the need to keep personal and professional/school lives separate
- Individuals should not put themselves in a position where there is a conflict between the Trust and their personal interests
- Do not make any derogatory, defamatory, rude, threatening or inappropriate comments about the Trust, or anyone at or connected with the Trust
- Use social networking sites responsibly and ensure that neither their personal nor professional reputation, nor the Trust's reputation is compromised by inappropriate postings.

14.2 Inappropriate and unprofessional use of social media

It is important and expected that staff understand what inappropriate and unprofessional use of social media is and adhere to the following:

- Staff should not engage in activities involving social media which might bring the Trust of a specific school of the Trust, or any individual associated into disrepute
- Staff should not represent their personal views as those of Trust or any school with the Trust on any social medium
- Staff should not discuss personal information about other students, the Trust, any school of the Trust and the wider community they interact with on any social media
- Staff should not use social media and the internet in any way to attack, insult, abuse or defame students, their family members, colleagues, other professionals, other organisations or Trust
- Staff should not identify themselves as members of Trust or any school of the Trust in their personal web-space, unless specifically linked to an approved job role within the Trust community where it serves a purpose to professionally market the Trust or their school. This is to prevent information being linked with the Trust and its schools and to safeguard the privacy of staff members, students and parents and the wider school community
- Students should not have contact through any personal social medium with any member of staff. If students and members of the wider Trust or individual school community wish to communicate with staff, they should only do so through official Trust or individual school sites created for this purpose
- Photographs, videos, or any other types of images of students and their families or images depicting staff members, clothing with school logos or images identifying school premises should not be published on personal or public web space without prior permission from the Trust, except for reposting of approved marketing material
- Trust and individual schools e-mail addresses should not be used for setting up personal social media accounts or to communicate through such media.

15. Training

Newly appointed staff will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

By way of this training, all staff will be made aware that:

Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse and that children can abuse other children online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat group

- Sharing of abusive images and pornography
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on online safety at regular intervals, and at least annually.

Trustees and Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable.

Volunteers will receive appropriate training and updates, if applicable.

16. Technical Security

Systems across the trust will be managed a variety of ways, depending on how services are procured, but this will always be done in partnership with the trust, school leaders and school-based network managers to ensure every school meets recommended technical requirements.

To include:

- Responsibility for technical security resides with the trust and schools' leadership teams who may delegate activities to identified roles
- All users have clearly defined access rights to school technical systems and devices.
- 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.
- The administrator passwords for school systems are kept in a secure place, e.g. school safe.
- 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 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
- Software purchased by and used by the school is adequately licensed and the latest software updates (patches) are applied
- Staff members are not permitted to install software on a school-owned devices
- Systems are in place to control and protect personal data and data is encrypted at rest and in transit.

The Trust will implement appropriate cyber security measures, including the use of Multi-Factor Authentication (MFA) where available, particularly for administrative and remote access accounts. Staff will receive regular training to help them recognise and respond to phishing attempts, social engineering and other cyber threats. Where appropriate, approved password management solutions may be used to support the secure creation and storage of passwords. Backup arrangements will be regularly tested to ensure data can be successfully recovered following a cyber incident, system failure or loss of information. Schools will also maintain and periodically review incident response and recovery procedures to ensure that cyber security incidents can be managed effectively and services restored as quickly as possible.

If the school has an external technology provider, it is the responsibility of the school to ensure that the provider carries out all the online safety and security measures that would otherwise be the responsibility of the school. It is also important that the technology provider is fully aware of the school Online Safety Policy

17. Artificial intelligence (AI)

Generative Artificial Intelligence (AI) tools are becoming increasingly common in education and wider society. Staff, pupils, parents and carers may access AI-powered tools such as chatbots, image generators, search assistants and content creation platforms. AI can support teaching, learning, accessibility, creativity and administrative efficiency, but it also presents safeguarding, privacy, security and ethical risks.

SEEAT recognises the educational benefits of AI when used safely, responsibly and appropriately. The Trust also recognises that AI technologies can generate inaccurate, biased or misleading content and may be used inappropriately to create harmful material, spread misinformation or disinformation, facilitate bullying, harassment or abuse, or generate manipulated images, audio and video, including so-called "deepfakes".

Any use of AI to bully, harass, intimidate, impersonate, exploit or cause harm to another individual will be treated as a safeguarding concern and managed in accordance with the school's Behaviour Policy, Child Protection and Safeguarding Policy, and any other relevant procedures.

The Trust will ensure that any AI tool used within school is subject to appropriate consideration of safeguarding, privacy, data protection and educational suitability before implementation. Where necessary, schools will undertake risk assessments and consult relevant data protection processes before approving the use of new AI technologies. Staff must not input confidential, personal, safeguarding or sensitive information into public AI systems unless expressly authorised and supported by appropriate safeguards.

Where AI systems process personal data, schools will ensure appropriate data protection assessments and contractual safeguards are in place.

Staff must exercise professional judgement when using AI-generated content and remain responsible for the accuracy, appropriateness and quality of any materials, communications, assessments or resources used within the school. AI-generated outputs should be reviewed and verified before use.

Pupils will be taught to use AI tools critically and responsibly, including understanding the limitations of AI, recognising misinformation and manipulated content, evaluating the reliability of AI-generated outputs, protecting personal information and reporting concerns where AI is used in a harmful or inappropriate manner.

The Trust will keep developments in AI under regular review and ensure that filtering, monitoring and safeguarding arrangements continue to take account of emerging AI technologies and associated risks.

17.1 AI Governance

Schools must ensure all AI tools are reviewed and approved before use. Risk assessments where required, will be completed before deployment.

17.2 Staff Use of AI

Staff may only use approved AI tools and must not enter confidential, personal, safeguarding or special category data into public AI systems. Outputs must always be reviewed for accuracy and appropriateness.

17.3 Pupil Use of AI

Pupils may use approved AI tools for educational purposes under appropriate supervision. Pupils will be taught to critically evaluate AI-generated content and recognise inaccuracies, bias, misinformation and manipulated content.

17.4 AI Safeguarding Risks

Schools recognise risks associated with:

- Deepfakes
- AI-generated bullying
- Synthetic images
- Impersonation
- Misinformation and disinformation
- Harmful chatbot interactions

Incidents will be managed in accordance with safeguarding and behaviour procedures.

17.5 Filtering and Monitoring of AI

The Trust will ensure that filtering and monitoring arrangements consider AI-generated content and evolving AI services when reviewing online safety risks.

18. Filtering and Monitoring

Each school within the trust will have its own unique demands and use of the internet.

However, all schools must ensure they appropriately safeguard staff and pupils through an effective online filtering and monitoring regime.

All schools are required to put in place strengthened measures to protect children from harm online, which includes, for example, cyber bullying, pornography, violence, substance misuse, self-harm, suicide, and the risk of radicalisation.

One of the ways we achieve this is by making sure we have effective device monitoring in place. Any search for content which is illegal or on the school block list will be identified on the daily reports received by the school.

Alerts are received in two ways. Live alerts will immediately notify the DSL (or other delegated appropriate adult) of searches for sites with illegal content, or that pose a risk, or perceived risk to pupil or adult safety made by pupils. The same routine applies, but instead notifies the head teacher of searches made by adults.

All schools within the Trust must ensure that internet systems are robust and appropriate for use. All schools are required to follow the Trust guidance below.

The filtering and monitoring provision across the Trust is agreed by senior leaders, governors and the SEEAT IT Manager, any external Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents and behaviour's.

Day-to-day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility

Filtering and monitoring provision is reviewed at least annually by the Trust, senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider where appropriate.

Checks on the filtering and monitoring system are carried out by the IT Manager with the involvement of a senior leader, the Designated Safeguarding Lead, and a governor, particularly when a safeguarding risk is identified, when there is a change in working practice, e.g. remote access, bring your own device (BYOD) or new technology is introduced.

18.1 Filtering

It is important to recognise that no filtering system can be 100% effective. It must be supported with good teaching and learning practice, effective supervision, and vigilance.

The filtering system is a tool used to support and inform the broader safeguarding provision in our schools.

- 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 [Appropriate filtering](#).
- 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. Staff, pupils, and visitors know how to raise a concern
- There is a clear process in place to deal with, and log, requests/approvals for filtering changes ([see Appendix for more details](#)).
- Filtering logs are reviewed daily during term time and alert the Designated Safeguarding Lead, and those designated to support the DSL to breaches of the filtering policy (by pupils), which are then acted upon.
- Filtering logs are reviewed daily during term time and alert the Head teacher, and those designated in their absence to breaches of the filtering policy (by staff), which are then acted upon.

- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and distinct groups of users: staff, learners, and Trust members)
- younger learners will use child friendly/age-appropriate search engines
- Where a school allows mobile devices that access the internet through the school network, content is managed in the same way as for school owned devices.

18.2 Illegal Online Content

Schools will ensure that access to illegal content is blocked and that filters for illegal content cannot be disabled. Specifically, that the filtering providers:

- are Internet Watch Foundation (IWF) members and use IWF services to block access to illegal Child Sexual Abuse Material (CSAM)
- Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'

18.3 Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, the school must be satisfied that their filtering system manages the following content (and web search)

Content	Explanatory Notes – content that:
Discrimination	Promotes the unjust or prejudicial treatment of people with protected characteristics of the Equality Act 2010
Drugs/ substance abuse	Displays or promotes the illegal use of drugs or substances
Extremism	Promotes terrorism and terrorist ideologies, violence or intolerance
Gambling	Enables gambling
Malware/ hacking	Promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
Pornography	Displays sexual acts or explicit images
Piracy and copyright theft	Includes illegal provision of copyrighted material
Self-harm	Promotes or displays deliberate self-harm (including suicide and eating disorders)
Violence	Displays or promotes the use of physical force intended to hurt or kill

Note: This list should not be considered an exhaustive list

The retention of logfile (Internet history), as the data controller, the schools understand their filtering providers data retention policies including the duration to which all data is retained and have associated data sharing agreements. Logfiles (Internet history) should include the identification of individuals and/or devices.

18.4 Filtering System Features

Considering the context of each school safeguarding needs, schools will consider how their filtering system meets the following principles:

- Context appropriate differentiated filtering, based on age, vulnerability, and risk of harm – also includes the ability to vary filtering strength appropriate for staff
- Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, for example VPN, proxy services and DNS (Domain Name System) over HTTPS
- Control – has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content. Any changes to the filter system are logged enabling an audit trail that ensure transparency and that individuals are not able to make unilateral changes
- Contextual Content Filters – in addition to URL or IP based filtering, the extent to which (http and https) content is analysed as it is streamed to the user and blocked, this would include AI generated content. For example, being able to contextually analyse text on a page and dynamically filter
- Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking
- Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard
- Identification - the filtering system should have the ability to identify users
- Network level - filtering should be applied at 'network level' i.e., not reliant on any software on user devices whilst at school (recognising that device configuration/software may be required for filtering beyond the school infrastructure)
- Remote devices – with many children and staff working remotely, the ability for school owned devices to receive the same or equivalent filtering to that provided in school
- Reporting mechanism – the ability to report inappropriate content for access or blocking
- Reports – the system offers clear historical information on the websites users have accessed or attempted to access
- Safe Search – the ability to enforce 'safe search' when using search engines

18.5 Filtering Test

Note: Filtering should be tested at least half termly, and in response to concerns, system failures and risks identified by the DSL and IT Lead. TestFiltering.com works by polling test pages to determine if the filtering system is blocking access to

- Illegal Child Sexual Abuse Material
 - Unlawful Terrorist Content
 - Adult Content
 - Additionally, the utility will test if any filters exist to filter offensive language.
- Testing must be recorded, including the test outcome.

18.6 Monitoring

Day-to-day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective.

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.
- Live monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored
- Daily monitoring reports are reviewed may inform on-line safety teaching and raise awareness contextual safeguarding and latest trends and interests
- 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
- Schools observe the [DfE Filtering and Monitoring Standards for Schools](#) and protects users and school systems through an appropriate blend of strategies, which 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 the DSL and senior leaders
 - pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
 - Trust and school technical staff regularly monitor and record the activity of users on the school technical systems

- use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s).

Appendix 1 - Links with other policies

The SEEAT On-line Safety Policy links to the policies listed below. Please follow the link for further information.

Policies
SEEAT Attendance Policy 2026
Behaviour Policy (local)
SEEAT Statement of Intent and Guiding Principles for Behaviour
Complaints Procedure
Equality and Diversity Policy
Health and Safety Policy
Online Safety Policy 2026
Relationships and Sex Education Policy 2026
Staff Code of Conduct
Safer Recruitment Policy
SEEAT Suspensions and Permanent Exclusions Policy 2026
SEEAT Supporting Pupils with Medical Conditions Policy 2026
Whistleblowing Policy

Appendix 2 – Appropriate use Agreements

EYFS (Early Years Foundation Stage) and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS
Name of pupil:
When I use the school's ICT systems (like computers) and get onto the internet in school I will: ● Ask a teacher or adult if I can do so before using them ● Only use websites that a teacher or adult has told me or allowed me to use ● Tell my teacher immediately if: ▪ I click on a website by mistake ▪ I receive messages from people I do not know ▪ I find anything that may upset or harm me or my friends ● Use school computers for schoolwork only ● I will be kind to others and not upset or be rude to them ● Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly ● Only use the username and password I have been given ● Try my hardest to remember my username and password ● Never share my password with anyone, including my friends ● Never give my personal information (my name, address, or telephone numbers) to anyone without the permission of my teacher or parent/carer ● Save my work on the school network ● Check with my teacher before I print anything ● Log off or shut down a computer when I have finished using it, I agree that the school will monitor the websites I visit and that there will be consequences if I do not follow the rules.
Signed (pupil): Date:
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these
Signed (parent/ carer): Date:

Appendix 2.1

KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS
Name of pupil:
I will read and follow the rules in the acceptable use agreement policy When I use the school's ICT systems (like computers) and get onto the internet in school I will: • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address, or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I am finished working on it.
I will not: • Access any inappropriate websites including social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails ▪ Log in to the school's network using someone else's details ▪ Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
If I bring a personal mobile phone or other personal electronic device into school: • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
Signed (pupil): Date:
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these
Signed (parent/ carer): Date:

Appendix 2.2

Acceptable use agreement (staff, trustees, governors, volunteers, and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS
Name of staff member/governor/volunteer/visitor:
When using the school/ Trusts ICT systems and accessing the internet in a school, or outside of SEEAT premises on a work device (if applicable), I will not: ● Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal, or pornographic nature (or create, share, link to or send such material) ● Use them in any way which could harm the school's reputation ● Access social networking sites or chat rooms ● Use any improper language when communicating online, including in emails or other messaging services ● Install any unauthorised software, or connect unauthorised hardware or devices to the school's network ● Share my password with others or log in to the school's network using someone else's details ● Share confidential information about specific schools or the Trust, its pupils or staff, or other members of the community ● Access, modify or share data I am not authorised to access, modify or share ● Promote private businesses, unless that business is related directly to a school or the Trust
I will only use the school/ Trusts ICT systems and access the internet in school/ SEEAT premises or outside of the school/ premises on a work device, for educational purposes or to fulfill my role's duties. I agree that the school/ Trust will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside of the school/ Trust, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil or staff member informs me, they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.
Signed (staff member/governor/volunteer/visitor): Date:

Appendix 3 – Audit tools

South East Essex Academy Trust (SEEAT)



Filtering and Monitoring Checklist

In line with the [DfE filtering and monitoring standards in schools and colleges](#), this checklist should be completed annually, or in response to a concern or risk being identified. Whilst not intended to be exhaustive, this resource can serve as a summary record of checks highlighted within the standards.

Last updated:	Date:	Name/Position:
---------------	-------	----------------

Roles and Responsibilities

Role	Responsibility	Name / Position
Responsible Governor	Strategic responsibility for filtering and monitoring and needs assurance that the standards are being met.	
Senior Leadership Team Member	• Responsible for ensuring these standards are met and: • procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of your provision • overseeing reports • Ensure that all staff: • understand their role • are appropriately trained • follow policies, processes, and procedures • act on reports and concerns	

Designated Safeguarding Lead	• Lead responsibility for safeguarding and online safety, which could include overseeing and acting on: • filtering and monitoring reports • safeguarding concerns • checks to filtering and monitoring systems	
IT Service Provider	• Technical responsibility for: • maintaining filtering and monitoring systems • providing filtering and monitoring reports • completing actions following concerns or checks to systems	

Reviewing your filtering and monitoring provision

Filtering System	
Filtering Provider and System	
Date Procured	
Date last reviewed	

Monitoring System	
Monitoring Provider and System	
Date Procured	
Date last reviewed	

Review Team [should be conducted by members of the senior leadership team, the Designated Safeguarding Lead (DSL), and the IT service provider and involve the responsible governor]	
Review Date	
Previous Review Date	
Link to last review	
Review Checklist	

the risk profile of your pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL (English as an Additional Language))	
what your filtering system currently blocks or allows and why	
any outside safeguarding influences, such as county lines	
any relevant safeguarding reports	
the digital resilience of your pupils	
teaching requirements, for example, your RHSE and PSHE curriculum	
the specific use of your chosen technologies, including Bring Your Own Device (BYOD)	
what related safeguarding or technology policies you have in place	
what checks are currently taking place and how resulting actions are handled	

all staff know how to report and record concerns	
filtering and monitoring systems work on new devices and services before release to staff / pupils	
blocklists are reviewed and they can be modified in line with changes to safeguarding risks	

Recommendations / Mitigating Actions	

Data Protection Impact Assessment

Schools and colleges that have a technical monitoring system will need to conduct their own Data Protection Impact Assessment (DPIA) and review the privacy notices of third-party providers

Link to DPIA	
Conducted by	

Date conducted	
----------------	--

Regular Reports

Type of Report	Filtering / Monitoring
Producer of report	
Recipient of report	
Frequency of report	

Monitoring data is received in a format that your staff can understand	
Users are identifiable to the school / college, so concerns can be traced back to an individual, including guest accounts	

System Checks

Filtering System				
Date checked				
Checks conducted by				
Device	Location	Logged in as	Check Conducted	Result

Appendices 3.1

On-line safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/ No Add comments if necessary
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors, and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendices 3.2

On-line Safety Incident Report Log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident