Online Safety and Social Networking Policy

Sturry CE Primary School

Reviewed September 2026

The Stour Academy Trust

The Board of Trustees reviews and approves this policy every year. It may, however, review this policy earlier than this if the government produces new regulations, or if it receives recommendations on how this policy might be improved.

This policy must be read in line with the Remote Learning Policy

Date agreed and ratified by The Board of Trustees: September 2026

As the sponsor school of The Stour Academy Trust, we promote collaboration in order to continue the growth and development of God's children. We are driven by our commitment to the well-being and education of all, enabling us to flourish and become life-long learners.

Through the miracle of Jesus feeding the 5000, we trust that sharing all we have will provide for all through the power of God's love.

This has been adapted to help the children understand our Christian vision:

We work together and share the best of ourselves to help everyone around us flourish in every way to become life-long learners. Through the miracle of Jesus feeding the 5000, we trust that sharing all we have will provide for all through the power of God's love.

Contents

Please note that any reference in this policy to 'School' refers to all academies within the Trust.

1. Creating an online safety ethos
1.1. Aims, purpose and policy scope.
1.2. Writing and reviewing the online safety policy
1.3. Key responsibilities of the community
1.3.1. Key responsibilities of the management team
1.3.2. Key responsibilities of the online safety/designated safeguarding lead
1.3.3. Key responsibilities of staff
1.3.4. Additional responsibilities of staff managing the technical environment
1.3.5. Key responsibilities of children and young people
1.3.6. Key responsibilities of parents/carers
2. Online communication and safer use of technology
2.1. Managing the website
2.2. Publishing images online
2.3. Managing email
2.4. Official video conferencing and webcam use
2.5. Appropriate safe classroom use of the internet and associated devices
2.6. Publishing Pupils Images and Work and storage of images

2.7. AI use section

3. Social media policy

4. Use of personal devices and mobile phones

4.1. Rationale regarding personal devices and mobile phones

4.2. Expectations for safe use of personal devices and mobile phones

4.3. Children use of personal devices and mobile phones

4.4. Staff use of personal devices and mobile phones

4.5. Visitors use of personal devices and mobile phones

5. Policy decisions

5.1. Internet use within the community

5.2. Authorising internet access

6. Engagement approaches

6.1. Engagement of children and young people

6.2. Engagement of children and young people who are considered to be vulnerable.

6.3. Engagement and education of staff

6.4. Engagement and education of parents/carers

7. Managing information systems

7.1. Managing personal data online

7.2. Security and managing information systems.

7.3. Filtering decisions

8. Responding to online incidents and concerns - Procedures for responding to specific online incidents or concerns (including sharing nudes and semi nudes, online child sexual abuse, indecent image of children, radicalisation, and cyberbullying)

1. Creating an Online Safety Ethos

1.1 Aims, purpose and policy scope.

- This online safety policy has been written by The Stour Academy Trust, involving staff, learners, and parents/carers, building on the Kent County Council online safety policy template, with specialist advice and input as required.
- It takes into account the DfE statutory guidance 'Keeping Children Safe in Education', Early Years and Foundation Stage, 'Working Together to Safeguard Children', Kent Safeguarding Children Multi-Agency Partnership (KSCMP) procedures, UK Safer Internet Centre guidance and the DfE filtering and monitoring standards.

The Stour Academy Trust believes that online safety is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, mobile phones, smart watches or games consoles. This includes emerging technologies such as wearable devices, smart

assistants, artificial intelligence (AI) tools, virtual reality systems and other internet-connected technologies that may collect, process or transmit data. It is essential that children are safeguarded from potentially harmful and inappropriate material or behaviours online. The Trust will adopt a whole school approach to online safety which will empower, protect, and educate our pupils and staff in their use of technology, and establish mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The Stour Academy Trust identifies that the internet and information communication technologies are an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.

The Stour Academy Trust has a duty to provide the school community with quality Internet access to raise education standards, promote pupil achievement, support professional work of staff, and enhance the schools' management functions. The Stour Academy Trust also identifies that with this there is a clear duty to ensure that children are protected from potential harm online.

The purpose of The Stour Academy Trust online safety policy is to:

- Safeguard and protect all members of The Stour Academy Trust community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

The Stour Academy Trust identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate, or harmful material. For example, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **Contact:** being subjected to harmful online interaction with other users. For example, peer to peer pressure, commercial advertising and adults posing as children 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. For example, making, sending, and receiving explicit images (e.g., consensual, and non-consensual sharing of nude and semi-nude images or videos) and/or pornography or other explicit images and online bullying.
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

The Stour Academy Trust has appropriate mobile and smart technology and image use policies in place, which are shared and understood by all members of the community. These policies can be found in the staff room, staff intranet and school website.

This policy applies to all staff including the Board of Trustees and members, teachers, support staff, external contractors, visitors, volunteers, and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.

This policy applies to all access to the internet and use of information communication devices including personal devices or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptop, iPad, or mobile phone.

This policy must be read in conjunction with other relevant school policies including (but not limited to) Child Protection and Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy, Mobile Phone / Smart Technology Policy, Data Protection Policy, Staff Code of Conduct, Acceptable Use Policy, Allegations Against Staff Policy, Complaints Policy and Remote learning Policy.

1.2 Writing and reviewing the online safety policy.

The Stour Academy Trust online safety policy has been written by the school, involving staff, pupils, and parents/carers, building on the KCC online safety policy template with specialist advice and input as required.

The Stour Academy Trust will ensure online safety is considered as a running and interrelated theme when devising and implementing our policies and procedures, and when planning our curriculum, staff training, the role and responsibilities of the DSL and parental engagement.
The policy has been approved and agreed by the Senior Leadership Team and the Board of Trustees.

The school has appointed a member of the leadership team as the online safety lead.

Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. This will cover the potential risks posed to learners (Content, Contact, Conduct and Commerce) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues, or other members of the community.

The schools' online safety policy and its implementation will be reviewed at least annually or sooner if required.

The Trust Online Safety Coordinators are Claire Jobe, Stella Schâringer and Vicki Acors

The Trust Designated Safeguarding Lead (DSL) is Rachael Howell

Individual school Designated Safeguarding leads are: -

School	Designated Safeguarding Lead (DSL)
Adisham CE Primary School	Sophie Metcalf
Chilmington Green Primary School	Tamsin Mobbs
Finberry Primary School	Sarah Martin
Water Meadows Primary School	Benjamin Martin
Lansdowne Primary School	Rachel Sullivan
Richmond Primary School	Lesley Conway

Sturry CE Primary School	Michelle Mannings
Thistle Hill Academy	Rebecca Handebeaux
St Crispin's Infant's School	Victoria Acors

1.3 Key responsibilities of the community

Rachael Howell, Claire Jobe, Stella Schâringer and Vicki Acors, members of the senior leadership team and Simon O'Keefe Board Trustee, are responsible for ensuring that our school has met the DfE Filtering and monitoring standards for schools and colleges.

Our Board of Trustees has overall strategic responsibility for our filtering and monitoring approaches, including ensuring that our filtering and monitoring systems are regularly reviewed, and that the leadership team and relevant staff have an awareness and understanding of the appropriate filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.

Our senior leadership team is responsible for

- procuring filtering and monitoring systems.
- documenting decisions on what is blocked or allowed and why.
- reviewing the effectiveness of our provision.
- overseeing reports.
- ensuring that all staff understand their role, are appropriately trained, follow policies, processes and procedures and act on reports and concerns.
- ensuring the DSL and IT Lead have sufficient time and support to manage their filtering and monitoring responsibilities.

1.3.1 Key responsibilities of the Trust are:

- Developing, owning, and promoting the online safety vision and culture to all stakeholders in line with national and local best practice recommendations with appropriate support and consultation throughout the school community
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.
- Supporting the online safety lead in the development of an online safety culture within the setting
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety.
- To ensure that suitable, age-appropriate, and relevant filtering is in place to protect children from inappropriate content (including extremist material) to meet the needs of the school community and ensuring that the filtering and school network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date, and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- Making appropriate resources available to support the development of an online safety culture.
- Taking responsibility for online safety incidents and liaising with external agencies as appropriate
- Receiving and regularly reviewing online safety incident logs and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local, and national support.

- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To work with and support technical staff in monitoring the safety and security of schools' systems and networks.
- To ensure that the Designated Safeguarding Lead (DSL) works in partnership with the online safety (e-safety) lead.
- Vulnerable Learners **-** The Stour Academy Trust recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss. The Stour Academy Trust will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners. The Stour Academy Trust will seek input from specialist staff as appropriate, including the SENDCO, Child in Care Designated Teacher.

- The IT service support has technical responsibility for:
    - maintaining filtering and monitoring systems.
    - providing filtering and monitoring reports.
    - completing technical actions identified following any concerns or checks to systems.
    - working with the senior leadership team and DSL to procure systems, identify risks, carry out reviews, and carry out checks.

1.3.2 Key responsibilities of the designated safeguarding/online safety lead are:

- Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate
- any filtering and monitoring reports
- any child protection or safeguarding concerns identified.
- checks to filtering and monitoring system.
- Keeping up to date with current research, legislation, and trends
- Coordinating participation in local and national events to promote positive online behaviour, e.g., Safer Internet Day
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Work with the Trust lead for data protection and data security to ensure that practice is in line with legislation.
- Maintaining an online safety incident/action log to record incidents and actions taken as part of each schools safeguarding recording structures and mechanisms.
- Monitor the Trust's online safety incidents to identify gaps/trends and update the education response to reflect need and to report to SLT, Board of Trustees and other agencies as appropriate.
- Liaising with the local authority and other local and national bodies as appropriate
- Reviewing and updating online safety policies, Acceptable Use Policies (AUPs), and other procedures on a regular basis (at least annually) with stakeholder input
- Ensuring that online safety is integrated with other appropriate school policies and procedures.

1.3.3 Key responsibilities of staff are:

- Contributing to the development of online safety policies
- Reading the Acceptable Use Policies (AUPs) and adhering to them
- Taking responsibility for the security of Trust systems and data
- Having an awareness of online safety issues, and how they relate to the children in their care.

- Modelling good practice in using new, emerging technologies, and demonstrating an emphasis on positive learning opportunities rather than focusing on negatives
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern, and taking appropriate action by working with the designated safeguarding lead
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site
- Taking personal responsibility for professional development in this area.
- All members of staff are provided with an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring as part of our induction process, and in our child protection staff training.
- Staff will receive appropriate training and updates to help them recognise signs of online harm, including cyberbullying, online exploitation, harmful online communities, and emerging risks associated with new technologies.
- Understanding emerging safeguarding risks associated with artificial intelligence tools, wearable technology, and synthetic media (e.g. manipulated images or “deepfakes”) and reporting concerns in line with safeguarding procedures.

1.3.4. Additional responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on Trust-owned devices.
- Ensuring that the Trust’s filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the online safety lead and DSL.
- Ensuring that the use of the setting’s network is regularly monitored in order that any deliberate or accidental misuse can be reported to the online safety lead and DSL.
- Report any breaches or concerns to the Designated Safeguarding Lead and leadership team and together ensure that they are recorded on the Online Safety Incident Log, and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the online safety lead and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.

1.3.5 Key responsibilities of children and young people are:

- Contributing to the development of online safety policies
- Reading the Acceptable Use Policies (AUPs) and adhering to them
- Respecting the feelings and rights of others both on and offline
- Seeking help from a trusted adult if things go wrong and supporting others that may be experiencing online safety issues.
- Pupils have a responsibility to follow this policy to report and record any filtering or monitoring concerns.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology and behaving safely and responsibly to limit those risks.

1.3.6. Key responsibilities of parents and carers are:

- Reading the Trust Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home
- Role modelling safe and appropriate uses of new and emerging technology.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the Trust, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Parents/carers have a responsibility to follow this policy to report and record any filtering or monitoring concerns.

2. Online Communication and Safer Use of Technology

2.1 Managing the school/setting website.

- The Trust will ensure that information posted on the school websites meets the requirements as identified by the Department for Education
- The contact details on the website will be the school address, email, and telephone number. Staff or pupils' personal information will not be published.
- The Head Teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- Each schools' website will comply with the schools' guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

2.2 Publishing images and videos online

- The Trust will ensure that all images are used in accordance with the Trust image use policy.
- In line with the Trust image policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

2.3 Managing email.

- Pupils may only use Trust provided email accounts for educational purposes.
- All members of staff are provided with a specific Trust email address to use for any official communication. This follows the format of full forename.surname@stouracademytrust.org.uk – e.g., Liz Brown would be elizabeth.brown@stouracdemytrust.org.uk
- The use of personal email addresses by staff for any official school/setting business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods.
- Members of the school community must immediately tell the DSL if they receive offensive communication, and this should be recorded in the school online safety incident log.

- Sensitive or personal information will only be shared via email in accordance with data protection legislation.
- Access in school to external personal email accounts may be blocked.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on Trust headed paper would be.

2.4 Official videoconferencing and webcam use

- All videoconferencing equipment in the classroom will be switched off when not in use and where appropriate, not set to auto answer.
- Equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses will not be made available to other sites.
- Videoconferencing contact information will not be put on the school website.
- The equipment will be kept securely and if necessary, locked away when not in use.
- Trust videoconferencing equipment will not be taken off school premises without permission.
- Responsibility for the use of the videoconferencing equipment outside school time will be established with care.
- Staff will ensure that external video conference is suitably risk assessed and that accounts and systems used to access events are appropriately safe and secure.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.

Users

- Pupils will ask permission from a teacher before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- Parents and carers consent will be obtained prior to children taking part in videoconferences.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote-control pages.
- Unique log on and password details for the educational videoconferencing services will only be issued to members of staff and kept secure.

Content

- When recording a videoconference lesson, written permission will be given by all sites and participants. The reason for the recording must be given, and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material will be stored securely.
- If third party materials are to be included, the school will check that recording is acceptable to avoid infringing the third-party intellectual property rights.
- The Trust will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site, the school will check that they are delivering material that is appropriate for the class.

2.5 Appropriate and safe classroom use of the internet and associated devices

- The Trust's internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Pupils will use age and ability appropriate tools to search the Internet for content.

The following approved search tools are reviewed regularly and are approved for use by staff and pupils:

- Microsoft Edge and Google Chrome – these websites are monitored 24/7 and a report is generated daily by London Grid for Learning (LGfL) which is monitored by the Trust Network team.
- Internet use is a key feature of educational access, and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum.
- The Trust will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Supervision of pupils will be appropriate to their age and ability.
- At Early Years Foundation Stage and Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials which supports the learning outcomes planned for the pupils' age and ability
- Early years children, in particular, are vulnerable due to a natural curiosity around their own and others' body parts and are the easiest to manipulate and coerce as they do not have the developed boundaries of older children. They may exhibit unhealthy attachments to screens, use inappropriate language and terminology and form inappropriate friendships with people online who they truly believe are friends. If privacy settings are not at the highest possible, they can inadvertently share personal information, images taken of themselves or held on the device, and/or financial information and purchases – the Brook traffic light tool can help practitioners to determine whether sexual behaviour is normal healthy sexual development or harmful behaviour which is a cause for concern.
- In our Early Years Foundation Stage (EYFS) curriculum, we prioritise online safety as an essential component of our educational approach. We utilise Project Evolve, which aligns with UKCIS (UK Council for Internet Safety) guidelines and is integrated into our online teaching framework.

Resources available for early years settings to use for education.

Childnet: Storybooks for early years and KS1 pupils

Smartie the Penguin

Digiduck Stories

Thinkuknow:

Resources for early years and KS1 pupils from NCA-CEOP

- At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools, and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.
- All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole school/setting requirement across the curriculum.

- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

All children take part in weekly online safety lesson with Project Evolve. The Project EVOLVE toolkit is based on the UKCIS framework “Education for a Connected World” (EFACW). This framework covers knowledge, skills, behaviours and attitudes across eight strands of our online lives from early years right through to eighteen. These outcomes or competencies are mapped to age and progress. The statements guide educators to the areas that they should be discussing with children as they develop their use of online technology.

Pupils will be taught, in an age- and ability-appropriate way, to critically evaluate online content and understand that not everything they see, read or hear online is accurate or trustworthy. This will include learning about misinformation, disinformation, manipulated content, AI-generated material, deepfakes, algorithms, recommendation systems and the ways in which online platforms can influence opinions, behaviour and wellbeing. Pupils will be supported to recognise harmful or misleading content, understand how online influence can affect decision-making, and know how and when to seek help or report concerns to a trusted adult, the Designated Safeguarding Lead, CEOP or another appropriate reporting route.

2.6 Publishing Pupil’s Images and Work and Storage of Images

On a child’s entry to the school, all parents / carers will be asked to give permission to use their child's work / image (photographic, audio and video) for promotional and in-school purposes. This includes school displays, schoolbooks, the school website, The Stour Academy Trust website, any social media sites used by the School/Trust e.g., Facebook/Twitter/YouTube, any communication software used by the School/Trust e.g., Arbor Parent Portal, any printed or digital promotional material, local/national media - both in print and online.

- The consent form is considered valid for the entire period that the child attends a school unless there is a change in the child’s circumstances where consent could be an issue. e.g., divorce of parents, custody issues etc.
- Parents/carers may withdraw permission in writing at any time.
- Email and postal addresses of pupils will not be published.

2.7 Use of Artificial Intelligence Tools

The Trust recognises that artificial intelligence (AI) tools are increasingly integrated into online platforms and applications used by pupils and staff.

AI tools must not be used to:

• record or analyse classroom conversations
• process or store personal data relating to pupils, staff or families
• generate content that impersonates members of the school community
• produce manipulated or synthetic images or recordings of pupils or staff

AI tools may only be used where they have been reviewed and approved by the Trust and comply with safeguarding, data protection and curriculum expectations.

Staff must ensure that pupils understand how AI-generated content may be inaccurate, misleading or harmful and will support pupils in developing critical awareness of AI-generated media.

Unapproved AI tools must not be used to collect, input, process, store, analyse or share any personal data relating to pupils, staff, parents, carers or family members. Staff must not use AI tools, transcription services, recording functions or meeting-summary features to record, transcribe, summarise or analyse

safeguarding discussions, behaviour incidents, child protection concerns, disciplinary matters, complaints, parental meetings, pupil support discussions or any other confidential meeting, unless the tool has been formally approved by the Trust and its use has been risk assessed as compliant with safeguarding, confidentiality and data protection requirements.

3. Social Networking Policy

Social Networking Policy - Parents

Overview

Social networking sites such as Facebook, Twitter and Instagram are now widely used. This type of media allows people to communicate in ways that were not previously possible that can positively enhance means of communication. The Trust recognises that most stakeholders use this in a positive and responsible manner. However, for a minority, such sites can be inappropriately used as a means of expressing negative or offensive views about the school within the Trust and their staff instead of approaching the school where the vast majority of concerns are easily dealt with and resolved. This document sets out the Trust's approach to parental use of such sites and sets out the procedures we will follow and action we may take when we consider that parents have used such facilities inappropriately. When we have referred to "parent" in this document, we also include carers; relatives; or anyone associated with the Trust.

Objectives

The purpose of this policy is to:

- Encourage social networking sites to be used in a beneficial and positive way by parents.
- Safeguard pupils, staff and anyone associated with the school from the negative effects of social networking sites.
- Safeguard the reputation of each school within the Trust from unwarranted abuse on social networking sites.
- Clarify what each school considers to be appropriate and inappropriate use of social networking sites by parents.
- Set out the procedures each school will follow where it considers parents have inappropriately or unlawfully used social networking sites to the detriment of the school, its staff or its pupils, and anyone else associated with the Trust.
- Set out the action the Trust will consider taking if parents make inappropriate use of social networking sites.

Appropriate use of social networking sites by parents

Social networking sites have potential to enhance the learning and achievement of pupils and enable parents to access information about their school and provide feedback efficiently and easily. In addition, the Trust recognises that many parents and other family members will have personal social networking accounts, which they might use to discuss/share views about school issues with friends and acquaintances. As a guide, individuals should consider the following prior to posting any information on social networking sites about a school, its staff, its pupils, or anyone else associated with it:

- Is the social networking site the appropriate channel to raise concerns, give this feedback or express these views?
- Would private and confidential discussions with the school be more appropriate? E.g., if there are serious allegations being made/concerns being raised. Social media/internet sites should not be used to name individuals and make abusive comments about those people. Please contact the school to discuss any concerns you may have.

- Are such comments likely to cause emotional or reputational harm to individuals which would not be justified, particularly if the school has not yet had a chance to investigate a complaint?
- The reputational impact that the posting of such material may have to the Trust; any detrimental harm that the school may suffer as a result of the posting; and the impact that such a posting may have on pupils' learning.

Inappropriate use of social networking sites by parents

Although social networking sites may appear to be the quickest and easiest way to express frustrations or concerns about a School (and those associated with it), it is never appropriate to do so.

Where a parent has a concern, this must be made through the appropriate channels by speaking to the class teacher, the Headteacher of the school or the Chair of the Board of Trustees, so they can be dealt with fairly, appropriately, and effectively for all concerned. (See Complaints Policy)

The Trust considers the following examples to be inappropriate uses of social networking sites. (This list is non-exhaustive and intended to provide examples only):

- Making allegations about staff or pupils at a school or cyber-bullying
- Making complaints about the school or staff at the school
- Making defamatory statements about the Trust or staff at the school
- Posting negative/offensive comments about specific pupils/staff at the school
- Posting racist comments
- Posting comments which threaten violence.

Parents should also ensure that their children are not using social networking/internet sites in an inappropriate manner. It is expected that parents/carers explain to their children what is acceptable to post online. Parents/carers are also expected to monitor their children's online activity, including in relation to their use of social media.

Procedure the school will follow if inappropriate use continues:

In the event that any pupil or parent/carer of a child/ren being educated in The Stour Academy Trust is found to be posting libellous or defamatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site. All social network sites have clear rules about the content which can be posted on the site, and they provide robust mechanisms to report contact or activity which breaches this. The Trust will also expect that any parent/carer removes such comments immediately and will be asked to attend a meeting with the Headteacher of the appropriate school to discuss the breaking of the Home-School Agreement and the possible repercussions of such action.

If the parent refuses to comply with these procedures and continues to use social networking sites in a manner the school considers inappropriate, the school will consider taking the following action:

- Take legal advice and/or legal action where the information posted is defamatory in any way or if the circumstances warrant this.
- Set out the school's concerns to you in writing, giving you a warning and requesting that the material in question is removed.
- Contact the Police where the school feels it appropriate – for example, if it considers a crime (such as harassment) has been committed; or in cases where the posting has a racial element, is considered to be grossly obscene or is threatening violence.
- If the inappropriate comments have been made on a school website or online forum, the school may take action to block or restrict that individual's access to that website or forum.
- Contact the host/provider of the Social Networking site to complain about the content of the site and ask for removal of the information.

- Take other legal action against the individual.

Social Networking Policy – Staff

In the context of this policy “everyone” refers to members of staff, trustees, friends and anyone working in a voluntary capacity in the Trust.

Introduction

Social networking activities conducted online outside work, such as blogging (writing personal journals to publicly accessible internet pages), involvement in social networking sites such as Facebook and posting material, images or comments on sites such as You Tube can have a negative effect on an organisation’s reputation or image. In addition, The Stour Academy Trust has a firm commitment to safeguarding children in all aspects of its work.

This policy has been written to set out the key principles and code of conduct that we expect of all members of staff with respect to their responsibilities in connection with the use of social networking sites.

Key Principles

Everyone* at The Stour Academy Trust has a responsibility to ensure that they protect the reputation of each Academy within the Trust, and to treat all colleagues and members of the Trust with professionalism and respect.

It is important to protect everyone* at The Stour Academy Trust from allegations and misinterpretations which can arise from the use of social networking sites.

Safeguarding children is a key responsibility of all members of staff, and it is essential that everyone at The Stour Academy Trust considers this and acts responsibly if they are using social networking sites out of the Trust. Anyone working in the Trust either as a paid employee or volunteer must not communicate with pupils and ex-pupils via social networking and must not accept or initiate Facebook or any other social networking friend requests from pupils and ex-pupils enrolled at The Stour Academy Trust.

This policy relates to social networking outside work. Accessing social networking sites at work using Trust equipment is not permitted unless it is being used by designated staff for Trust publicity or promotion.

Aims

- To set out the key principles and code of conduct expected of all members of staff, trustees, friends and volunteers at The Stour Academy Trust with respect to social networking.
- To further safeguard and protect children and staff.

Code of Conduct for Everyone* at The Stour Academy Trust - Social Networking

The following are not considered acceptable at The Stour Academy Trust:

- The use of each School’s/Trust’s name, logo, or any other published material without written prior permission from the Chief Executive Officer. This applies to any published material including the internet or written documentation.
- The posting of any communication or images which links any schools within the Trust to any form of illegal conduct, or which may damage its reputation. This includes defamatory comments.
- The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of any School.

- The posting of any images of employees, children, trustees, or anyone directly connected with the Trust whilst engaged in School activities except by a designated person for agreed publicity use.

In addition to the above everyone* at The Stour Academy Trust must ensure that they:

- Do not make any derogatory, defamatory, rude, threatening, or inappropriate comments about the schools, or anyone at or connected with the Trust.
- Use social networking sites responsibly and ensure that neither their personal/ professional reputation, or the school's reputation is compromised by inappropriate postings.
- Are aware of the potential of on-line identity fraud and to be cautious when giving out personal information about themselves which may compromise their personal safety and security.
- Communication between pupils and adults should take place within clear and explicit professional boundaries.
- Should not share any personal information with a child or young person.
- All communications are transparent and open to scrutiny.
- Personal contact details including email, home or mobile numbers should not be given unless the need to do so is agreed by the Executive Headteacher or CEO
- Ensure that personal social networking sites are set to Private, and pupils are never listed as approved contacts.
- Never use or access social networking sites of pupils
- Not give their personal contact details to pupils, including their mobile telephone number
- Only use equipment e.g., mobile phones provided by the Trust to communicate with children, making sure that parents have given permission for this form of communication to be used.
- Recognise that text messaging should only be used as part of an agreed protocol and when other forms of communication are not possible.
- Not use internal or web-based communication channels to send personal messages to a child/young person.
- It is strongly recommended that Facebook friend requests not be initiated to or accepted from parents.
- Potential and Actual Breaches of the Code of Conduct.

In instances where there has been a breach of the above Code of Conduct, the following will apply:

- Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy this may result in action being taken under the Disciplinary Procedure. A breach of this policy will be considered a serious disciplinary offence which is also contrary to the Trust's ethos and principles.
- The Trustees will take appropriate action to protect the Trust's reputation and that of its staff, parents, trustees, children and anyone else directly linked to the Trust.

4. Use of Personal Devices, Mobile Phones and Smart Technology

4.1 Rationale regarding personal devices, mobile phones and smart technology

- The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of The Stour Academy Trust community to take steps to ensure that mobile phones and personal devices are used responsibly.
- The use of mobile phones and other personal devices by young people and adults will be decided by the school and covered in appropriate policies including the school Acceptable Use Policy
- The Stour Academy Trust recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers but requires that such technologies need to be used safely and appropriately within school.

4.2 Expectations for safe use of personal devices and mobile phones

- Electronic devices of all kinds that are brought into school are always the responsibility of the user. The Trust accepts no responsibility for the loss, theft or damage of such items. Nor will the Trust accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones, personal devices and smart technology are not permitted to be used in certain areas within a school site such as changing rooms, toilets and swimming pools.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the Trust community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- Members of staff will be issued with a school/work phone number and email address where contact with pupils or parents/carers is required.
- All members of The Stour Academy Trust community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
- All members of The Stour Academy Trust community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.
- All members of The Stour Academy Trust community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered offensive, derogatory or would otherwise contravene the school/settings policies.
- School/setting mobile phones and devices must always be used in accordance with the Acceptable Use Policy
- School/setting mobile phones and devices used for communication with parents and pupils must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.
- Where situations arise i.e., lockdown, the remote learning policy is implemented. Discussion will take place with a DSL regarding consideration and appropriateness of staff using their own devises to contact pupils and their parents/carers. If a school device is not available; the member of staff **will** withhold their mobile number when making contact. Parents/carers will need to ensure they answer phone calls from a private number. Arrangements will be made prior to this i.e. calls will be made at certain times each day or day of the week in agreement with the parent/carer.

4.3 Pupils use of personal devices, mobile phones, and smart technology

Pupil use of mobile phones, smart watches, wearable devices and other personal smart technology must follow the Trust Mobile Phone Policy and this Online Safety Policy. Devices may only be brought to school with agreed permission, such as for travel, medical, safeguarding or accessibility reasons, and must be switched off or stored securely unless authorised. Unauthorised or inappropriate use, including recording, photographing, filming, livestreaming, messaging or internet access, will be managed through the Behaviour Policy, Mobile Phone Policy and safeguarding procedures. Any confiscation, searching or device examination must follow Trust procedures and take account of any safeguarding, medical or legal concerns.

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- All use of mobile phones and personal devices by children will take place in accordance with the acceptable use policy.
- The Trust Policy strongly discourages pupils from bringing mobile phones to school. However, we do appreciate that some parents feel more at ease knowing they can be contacted in the event of an emergency if a child walks home alone.

- If a pupil brings a mobile phone to school; the phone must remain switched off during the school day and kept in the school office.
- If a pupil is found by a member of staff to be using a mobile phone; the phone will be confiscated from the pupil and returned at the end of the day.
- The Stour academy Trust accepts no liability for the loss or damage to mobile phones or any devices which are brought into school.
- If a pupil needs to contact his/her parents/carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office. Exceptions may be permitted in exceptional circumstances on a case-by-case basis and as approved by the headteacher.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- Trust staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the schools' behaviour or bullying policy. The phone or device may be searched by a member of the Leadership team with the consent of the pupil or parent/carer.
- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, then the device will be handed over to the police for further investigation.

4.4 Staff use of personal devices, mobile phones, and smart technology

- Members of staff are not permitted to use their own personal phones or devices for contacting children, young people, and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this must be discussed with leaders/managers.
- Staff will not use personal devices such as mobile phones, tablets, or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
- Staff must not use personal devices or AI tools to record, transcribe or summarise meetings, lessons or safeguarding discussions involving pupils.
- Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities (exemptions of the above apply when situations arise i.e., lockdown and the Remote Learning Policy is implemented).
- To protect staff, it is recommended that all mobile phones are kept in a bag or locker during lessons. (This has now become a disciplinary action)
- Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
- Personal mobile phones or devices will not be used during breakfast and after-school provision unless permission has been given by a member of the Leadership Team in emergency circumstances.
- Microsoft Authenticator app will be used for two-factor authentication not mobile phones.
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the policy, then disciplinary action will be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, then the police will be contacted, and allegations will be responded to following the allegations management policy.

4.5 Visitors use of personal devices, mobile phones, and smart technology

- Parents/carers and visitors must use mobile phones, personal devices and smart technology in accordance with our acceptable use policy and other associated polices, including child protection.
- If visitors require access to mobile and smart technology, for example when working with learners as part of multi-agency activity, this will be discussed with the head teacher prior to use being permitted.
- Any arrangements regarding agreed visitors access to mobile/smart technology will be documented and recorded by the school. This may include undertaking appropriate risk assessments if necessary.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

4.6 Wearable, Recording and AI-Enabled Devices

- Wearable technology and AI-enabled devices (including smart glasses, smart watches, fitness trackers, AI recording devices, and similar technology) are considered personal smart devices and are subject to the same expectations as mobile phones.
- Devices that are capable of audio recording, video recording, image capture, live streaming, or continuous listening must not be worn or used on site unless explicitly authorised by the Headteacher or a member of the Leadership Team for a specific purpose.
- Wearable or AI-enabled devices must not be used to record, store, process, transmit, or analyse any data relating to children, staff, or visitors.
- Any unauthorised use of wearable or AI-enabled recording technology will be treated as a safeguarding concern and managed in line with the school's disciplinary and safeguarding procedures.

5. Policy Decisions

- Technology evolves and changes rapidly. The Stour Academy Trust is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites, and material emerging at a rapid pace.
- Emerging technologies will be examined for educational benefit and the Trust's leadership team will ensure that appropriate risk assessments are carried out before use in the Trust is allowed.
- The Stour Academy Trust will ensure that appropriate filtering systems are in place to prevent staff and pupils from accessing unsuitable or illegal content.
- The Stour Academy Trust will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a Trust computer or device.
- The Trust will audit technology use to establish if the online safety policy is adequate and that the implementation of the policy is appropriate. The policy will be revised following any national or local policy updates, any local concerns and/or any changes to our technical infrastructure.
- Methods to identify, assess and minimise online risks will be reviewed regularly by the Trust leadership team.
- Filtering decisions, internet access and device use by pupils and staff will be reviewed regularly by the Trust leadership team.
- The Trust recognises that emerging technologies such as artificial intelligence systems, wearable devices, immersive technologies and algorithm-driven platforms may introduce new safeguarding risks. The Trust will regularly review these technologies and undertake risk assessments before they are used within the school environment.

- The Trust will review developments in digital technology and update safeguarding procedures where new risks are identified.

5.1. Internet use throughout the wider school/setting community

- Each school will liaise with local organisations to establish a common approach to online safety.
- Each school will provide an Acceptable Use Policy for any guest/visitor who needs to access the school computer system or internet on site.

5.2. Authorising internet access

- The Stour Academy Trust will maintain a current record of all staff and pupils who are granted access to the Trust's electronic communications.
- All staff, pupils and visitors will read and sign the School Acceptable Use Policy before using any school ICT resources.
- Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

6. Engagement Approaches

6.1 Engagement and education of children and young people

- An online safety curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.
- Education about safe and responsible use will precede internet access.
- Pupils input will be sought when writing and developing school online safety policies and practices.
- Pupils will be supported in reading and understanding the school Acceptable Use Policy in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- Online safety will be included in the PSHE, RSE, Citizenship and Computing programmes of study covering both safe school and home use.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- Pupils will be taught how algorithms and recommendation systems used by online platforms can influence the content they see online and how to critically evaluate such content.
- The Trust recognises that online platforms use automated recommendation systems (algorithms) which may influence the content users see online. Pupils will be supported to understand how these systems work and how they may expose users to harmful, misleading or extreme content. Teaching will support pupils to critically evaluate online content and recognise how digital platforms are designed to maximise engagement.

6.2 Engagement and education of children and young people who are considered to be vulnerable

The Stour Academy Trust is aware that some children may be considered to be more vulnerable online due to a range of factors and will ensure that differentiated and ability appropriate online safety education is given, with input from specialist staff as appropriate (e.g., SENCO).

6.3 Engagement and education of staff

- The online safety policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of Trust safeguarding practice.
- To protect all staff and pupils, the Trust will implement Acceptable Use Policies which highlights appropriate online conduct and communication.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis.
- Members of staff with a responsibility for managing filtering systems or monitor ICT use will be supervised by the Leadership Team and will have clear procedures for reporting issues or concerns.
- The Trust will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within Trust. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

6.4 Engagement and education of parents and carers

- The Stour Academy Trust recognise that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- Parents' attention will be drawn to the school online safety policy and expectations in newsletters, letters, the school prospectus and on the school website.
- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use.
- Parents will be requested to read online safety information as part of the Home School Agreement
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on online safety will be made available to parents in a variety of formats.
- Parents will be encouraged to role model positive behaviour for their children online.

7. Managing Information Systems

7.1 Managing personal data online.

- Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 2018
- Staff are aware of their responsibility when accessing Trust data. Level of access is determined by the Data Protection Officer - Tommy Cullen COO and implemented by the Network Manager
- Any data taken off the Trust premises must be encrypted. (Advice must be sought from the Network Manager when doing this).
- Data can only be accessed and used on Trust computers, iPad or laptops. Staff are aware they must not use their personal devices for accessing any Academy, children, or pupil data.

7.2 Security and Management of Information Systems

- The security of the Trust information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.

- Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
- Portable media may not be used without specific permission followed by an anti-virus /malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The network manager will review system capacity regularly.
- The appropriate use of user logins and passwords to access the school network will be enforced for all but the youngest users.
- All users will be expected to log off or lock their screens/devices if systems are unattended.
- Each school will log and record internet use on all school owned devices.
- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.
- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.
- From Reception, all pupils are provided with their own unique username and private passwords to access school systems. Pupils are responsible for keeping their password private.
- We require staff and pupils to use STRONG passwords for access into our system.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers, or others.
- If you think your password may have been compromised or someone else has become aware of your password report this to The Stour Academy Trust IT Support.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the Trust networks and data, Arbor systems including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations, laptops, and iPads are not left unattended and are locked.
- Staff are advised to update their passwords every 42 days.
- Under no circumstances are staff allowed any other person to use their username and password (This could result in disciplinary action).

7.3 Filtering Decisions

The Stour Academy Trust will do all we reasonably can to limit children's exposure to online harms through school provided devices and networks and in line with the requirements of the Prevent Duty and KCSIE, we will ensure that appropriate filtering and monitoring systems are in place.

When implementing appropriate filtering and monitoring, The Stour Academy Trust will ensure that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

Whilst filtering and monitoring is an important part of our online safety responsibilities, it is only one part of our approach to online safety and we recognise that we cannot rely on filtering and monitoring alone to safeguard our pupils; effective safeguarding practice, robust policies, appropriate classroom/behaviour management and regular education/training about safe and responsible use is essential and expected.

Decision making and reviewing our filtering and monitoring provision.
When procuring and/or making decisions about our filtering and monitoring provision, our senior leadership team and IT Lead work closely with the DSL and the service provider. Decisions have been

recorded and informed by an approach which ensures our systems meet our trust specific needs and circumstances, including but not limited to our pupil risk profile and specific technology use.

Any changes to the filtering and monitoring approaches will be assessed by staff with safeguarding, educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.

Our Trust undertakes annual, monthly, and weekly reviews of our filtering and monitoring systems to ensure we understand the changing needs and potential risks posed to our community.
The DfE filtering and monitoring standards

In addition, our school undertakes regular checks on our filtering and monitoring systems, which are logged and recorded, to ensure our approaches are effective and can provide assurance to the Board of Trustees that we are meeting our safeguarding obligations.

Weekly checks are undertaken by the DSL/IT Lead with two members of staff present, undertaken in a location where confidentiality can be achieved, during working hours, when pupil's checks are logged/recorded, any technical concerns are flagged to the IT service provider and safeguarding concerns are actioned by the DSL etc.in line with this policy. Tech Checks are undertaken by the staff on a weekly ad hoc basis and recorded.

- Each school's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational, and safeguarding staff.
- Each school uses educational filtered secure broadband connectivity through the KPSN which is appropriate to the age and requirement of our pupils.
- Each school uses Light Speed filtering system which blocks sites that fall into categories which promotes discrimination or extremism, racial hate, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material of an illegal nature including child sexual abuse material (CSAM).
- Each school will ensure that age and ability appropriate filtering is in place whilst using school devices and systems to try and prevent staff and pupils from being accidentally or deliberately exposed to unsuitable content.
- Each school will work with KCC and the Schools Broadband team or broadband/filtering provider to ensure that filtering policy is continually reviewed.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead and will then be recorded and escalated as appropriate.
- The school filtering system of each school will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team
- All changes to any school filtering policy will be logged and recorded.
- The Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP and Police CyberAlarm immediately.
- The Stour Academy Trust is aware of its responsibility when monitoring staff communication under current legislation and takes into account the UK GDPR and the Data Protection Act 2018, The

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000 and Human Rights Act 1998.

- Staff and pupils are aware that Trust based email and internet activity can be monitored and explored further if required.
- The Trust does not allow pupils access to internet logs.
- The Trust uses management control tools for controlling and monitoring workstations.
- If staff or pupils discover an unsuitable site, the screen must be switched off / closed and the incident reported immediately to the class teacher.
- Pupils and staff are not permitted to download programs or files.
- Our filtering system is operational, up to date and is applied to all users, including guest accounts, all school owned devices and networks, and all devices using the school broadband connection.

Filtering breaches will be reported to the DSL and technical staff and will be recorded and escalated as appropriate and in line with relevant policies, including our child protection, acceptable use, allegations against staff and behaviour policies.

Parents/carers will be informed of filtering breaches involving their child.

Any access to material believed to indicate a risk of significant harm, or that could be illegal, will be reported as soon as it is identified to the appropriate agencies, including but not limited to the Internet Watch Foundation (where there are concerns about child sexual abuse material), Kent Police, NCA-CEOP or Kent Integrated Children's Services.

If staff are teaching topics which could create unusual activity on the filtering logs, or if staff perceive there to be unreasonable restrictions affecting teaching, learning or administration, they will report this to the IT Support who will liaise with the DSL and/or leadership team to advise on the correct procedure.

8. Responding to Online Incidents and Concerns

The Trust recognises that online safety incidents may occur outside of the school environment but can still have a significant impact on the wellbeing, safety or behaviour of pupils within school. Such incidents will be treated as safeguarding concerns where appropriate and managed in line with the Trust safeguarding procedures.

- All members of the Stour Academy Trust community will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.)
- The Designated Safeguarding Lead (DSL) will be informed of any online safety incidents involving child protection concerns, which will then be recorded.
- The Designated Safeguarding Lead (DSL) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.
- Complaints about Internet misuse will be dealt with under the Trust's complaints procedure.
- Complaints about online bullying will be dealt with under the Trust's anti-bullying policy and procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer)
- Pupils, parents, and staff will be informed of the Trust's complaints procedure.
- Staff will be informed of the complaints and whistleblowing procedure.
- All members of the Trust community will need to be aware of the importance of confidentiality and the need to follow the official Trust procedures for reporting concerns.

- All members of the Trust community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress, or offence to any other members of the school community.
- The Trust will manage online safety incidents in accordance with the Trust behaviour policy where appropriate.
- The Trust will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the Trust will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the Trust will contact the Education Safeguarding Team or Kent Police via 999 if there is immediate danger or risk of harm
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police
- If the Trust is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team
- If an incident of concern needs to be passed beyond the Trust, then the concern will be escalated to the Education Safeguarding Team to communicate to other schools/settings in Kent.
- Parents and children will need to work in partnership with the Stour Academy Trust to resolve issues**.**
- The Trust recognises that artificial intelligence tools can be used to create manipulated or synthetic media (sometimes referred to as “deepfakes”). If a member of the school community becomes aware of manipulated images, videos or recordings involving pupils, staff or members of the community, this will be treated as a safeguarding concern and reported to the Designated Safeguarding Lead. The Trust will respond to such incidents in line with safeguarding, behaviour and anti-bullying policies and may involve external agencies where appropriate.

Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- The Stour Academy Trust will ensure that all members of the community are aware of online child sexual abuse, including exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The Stour Academy Trust recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy)
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally
- We will ensure that the ‘Click CEOP’ report button is visible and available to learners and other members of our community on our school website.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
    - Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board’s procedures
    - If appropriate, store any devices involved securely.
    - Make a referral to Children’s Social Work Service (if required/appropriate) and immediately inform Kent police via 101, or 999 if a child is at immediate risk.
    - Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies)

    - Inform parents/carers about the incident and how it is being managed.
    - Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
    - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
    - Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Team and/or Kent Police
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the DSL (or deputy)
- If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

Online Sexual Violence and Sexual Harassment between Children

- Our setting has accessed and understood "guidance in part 5 of 'Keeping Children Safe in Education 2026' Child-on-Child sexual harassment and sexual violence.
- The Stour Academy Trust recognises that sexual violence and sexual harassment between children can take place online. Examples may include non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
    - Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.
- The Stour Academy recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- The Stour Academy Trust also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- The Stour Academy Trust will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies

- If content is contained on learner's electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
- Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- If appropriate, make a referral to partner agencies, such as Children's Social Service and/or the Police.
- If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
    - If a criminal offence has been committed, the DSL (or deputy) will discuss this with Kent Police first to ensure that investigations are not compromised.
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

Youth Produced Sexual Imagery ("Sexting")

- The Stour Academy Trust recognises youth produced sexual imagery (known as "sexting") or indecent imagery the legal term used to define nude or semi-nude images and videos of children and young people under the age of 18.
- 'sexting' is a term used by many adults, however some young people interpret sexting as 'writing and sharing explicit messages with people they know' rather than sharing images. Image-based sexual abuse is a term used when referring to the non-consensual sharing of nudes and semi-nudes. This is a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy)
- We will follow the advice as set out in the non-statutory UK Council for Internet Safety (UKCIS) full 2020 guidance: Sharing Nudes and Semi Nudes: Advised for education settings working with children and young people updated 11th March 2024 and KSCB guidance: "Responding to youth produced sexual imagery"
- The Stour Academy Trust will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We will not:
    - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
        - If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
    - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e., youth produced sexual imagery) and will not allow or request learners to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

- Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board's procedures
- Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Store the device securely.
    - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
- Carry out a risk assessment which considers any vulnerability of learners involved, including carrying out relevant checks with other agencies.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- Make a referral to Children's Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

Indecent Images of Children (IIOC)

- The Stour Academy Trust will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC)
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through Kent Police and/or the Education Safeguarding Team

- If made aware of IIOC, we will:
    - Act in accordance with our child protection policy and the relevant Kent Safeguarding Child Boards procedures
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent police or the LADO

- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:

    - Ensure that the DSL (or deputy) is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Report concerns, as appropriate to parents and carers.

- If made aware that indecent images of children have been found on the setting provided devices, we will:
    - Ensure that the DSL (or deputy) is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Inform the police via 101 (999 if there is an immediate risk of harm) and Children's Social Work Service (as appropriate)
    - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
    - Report concerns, as appropriate to parents and carers.

- If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:
    - Ensure that the Head Teacher is informed in line with our managing allegations against staff policy.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
    - Quarantine any devices until police advice has been sought.

Online Hate

- Online hate content, directed towards or posted by specific members of the community will not be tolerated at The Stour Academy Trust and will be responded to in line with existing policies, including anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Team and/or Kent Police

Responding to concerns regarding radicalisation or extremism online

The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils. Schools will need to highlight specifically how internet use will be monitored either here or within subsequent sections.

When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately, and action will be taken in line with the school safeguarding policy.

Responding to concerns regarding cyberbullying

- Cyberbullying, along with all other forms of bullying, of any member of the Stour Academy Trust community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.
- All incidents of online bullying reported will be recorded.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.
- If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools Online Safety ethos.

The Stour Academy Trust School Staff Code of Conduct for ICT

- To ensure that all members of staff are fully aware of their professional responsibilities when using information systems and when communication with pupils, you are asked to sign this code of conduct.
- Members of staff should consult the Trust Online-safety policy for further information and clarification.
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, personal digital assistance (PDAs), digital camera, email, social networking and that ICT use may also include personal ICT devices when used for Academy business.
- I understand that Academy information systems may not be used for private purposes without specific permission from the ICT Leader or CEO
- I understand that my use of Academy information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security, and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software of hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any instances of concern regarding children's safety to the Online Safety Coordinator and the Designated Safeguarding Lead.
- I will ensure that electronic communications with pupils including email are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I am aware that images and text posted on public sites may be viewed by pupils and their parents. I will strive to ensure that my professional status will not be affected by anything I post in the public domain.
- I will not discuss Academy issues on any social networking sites.
- I will promote Online-safety with students in my care and will help them to develop a responsible attitude to system use, communications, and publishing.
- I understand that breaches of this Code of Conduct may result in disciplinary action being taken.

The Stour Academy Trust may exercise its right to monitor the use of the Academy information systems and internet access, to intercept email and to delete inappropriate materials where it believes unauthorised use of the Academy information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood, and accept the Staff Code of Conduct for ICT:

Signed:

Name:

Date:

I have read, understood, and accept the Social Networking Policy:

Signed:

Name:

Date:

I confirm that this member of staff has read, understood, and accepted the Staff Code of Conduct for ICT and the Social Networking Policy:

Signed:

Headteacher:

Date: